HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto Fakultet/Sektion – Faculty	Laitos/Institution– Department	
Lääketieteellinen tiedekunta / psykologian ja logopedian osasto		
Tekijä/Författare – Author		
Heini Järviö		
Työn nimi / Arbetets titel – Title		
Ihminen osana tietoturvaa: persoonallisuus ja perusteltu toiminta tietoturvakäyttäytymisen taustalla		
Oppiaine /Läroämne – Subject		
Psykologia		
Työn laji/Arbetets art – Level	Aika/Datum – Month and year	Sivumäärä/ Sidoantal – Number of pages
Pro gradu -tutkielma	Toukokuu 2018	40

Tiivistelmä/Referat – Abstract

Tavoitteet. Kun tietoturva pettää, jopa yksi kolmesta tapahtumasta voi olla seurausta ihmisen toiminnasta, minkä takia teon ennustajien tunteminen on nykypäivänä eriarvoista. Tässä tutkimuksessa tavoitteena oli tarkastella, millaisia yksilön ja organisaation tekijöitä on sen taustalla, miten toimimme henkilökohtaisen ja organisaation tietojen suhteen. Kiinnostuksen kohteena oli mittausmalli, jossa perustellun toiminnan teoriaa (TRA) ja persoonallisuuden piirteitä tarkasteltiin tietoturvakäyttäytymisen ennustajina. TRA:ssa toiminnan vahvin ennustaja on intentio, jonka taustalla vaikuttavat asenne toimintaa kohtaan sekä subjektiiviset normit. Skenaarioasetelmaa hyödyntäen tavoitteena oli tarkastella, ennustaako TRA toimintaa myös konkreettisissa skenaariotilanteissa. Persoonallisuusteorioista kiinnostuksen kohteena olivat viisi suurta piirrettä sekä Dark Triad -piirteet, joista jälkimmäisen yhteyksistä tietoturvakäyttäytymiseen ei toistaiseksi ole juurikaan tutkimusta.

Menetelmät. Tutkimuksen aineisto (n=408) koostui Maanpuolustuskorkeakoulun sekä Helsingin yliopiston opiskelijoista. Osallistujat vastasivat kyselylomakkeeseen, jolla mitattiin persoonallisuutta ja TRA:n elementtejä. Lisäksi osallistujat saivat luettavakseen kolme skenaariota, joiden suhteen he arvioivat miten todennäköisesti toimisivat samalla tavalla (intentio) ja miten suhtautuivat tekoon (asenne). Tutkimuksen skenaariot oli jaettu kolmelle vaarallisuusasteelle, joista kukin vastaaja sai luettavakseen vain saman vaarallisuusasteen skenaarioita. Käytetyt persoonallisuusinventaarit olivat Short Five ja Short Dark Triad. Persoonallisuuden yhteyttä arvioihin skenaariotilanteissa tutkittiin regressioanalyysillä. Tutkimuksen mittausmallia arvioitiin polkuanalyysillä.

Tulokset ja johtopäätökset. Mittausmallin mukainen rakenne toteutui aineistoissa tietoturva-asenteen osalta silloin, kun esitettyjen skenaarioiden haitta oli vain vähäinen. TRA oli siis yhteydessä asenteisiin myös konkreettisessa tilanteessa. Eri persoonallisuuden piirteet olivat yhteydessä intentioihin ja asenteisiin. Kahdella Dark Triad -piirteellä oli positiivinen yhteys intentioon. Ekstroversio oli negatiivisesti yhteydessä sekä intentioon että asenteisiin. Lisäksi avoimuus oli positiivisesti yhteydessä asenteisiin, ja nämä yhteydet säilyivät mittausmalliin sisällytettyinä. Tämä tutkimus tarjosi lisätietoa persoonallisuuden yhteyksistä tietoturvakäyttäytymiseen sekä siihen, millaisia tekijöitä organisaatioissa tulisi ottaa huomioon tiedon turvaamiseksi.

Avainsanat – Nyckelord – Keywords
Tietoturvakäyttäytyminen, perustellun toiminnan teoria, Big Five, Dark Triad, skenaariomenetelmä

Säilytyspaikka – Förvaringställe – Where deposited
Helsingin yliopiston kirjasto – Helda / E-thesis (opinnäytteet) *ethesis.helsinki.fi*

Muita tietoja – Övriga uppgifter – Additional information
Ohjaajat: Petteri Simola (Puolustusvoimien tutkimuslaitos), Marjaana Lindeman (HY)

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto Fakultet/Sektion – Faculty	Laitos/Institution– Department
Faculty of Medicine / Department of psycholofy and logopedics	

Tekijä/Författare – Author
Heini Järviö

Työn nimi / Arbetets titel – Title
Human factors in information security – personality and reasoned actions behind information security behaviour

Oppiaine /Läroämne – Subject
Psychology

Työn laji/Arbetets art – Level	Aika/Datum – Month and year	Sivumäärä/ Sidoantal – Number of pages
Master's thesis	May 2018	40

Tiivistelmä/Referat – Abstract

Objectives. Even over one third of information security breaches are caused by human actions, which makes knowing the factors behind information security behaviour especially important in today's world. The objective of this study was to investigate what kind of individual and organisational factors affect the way we act with personal and organisational data. The research model of this study combined the Theory of Reasoned Action (TRA) and personality traits as predictors of information security behaviour. In TRA, the best predictor of an action is the intention to do it, which in turn is affected by the attitude towards the action and subjective norms. Scenario method was used to investigate if TRA predicts actions also in concrete scenarios The included personality theories were Big Five and Dark Triad theories, of which the latter has not yet been studied in information security research.

Methods. The data in this study was a sample of the students in the University of Helsinki and the National Defence University (N=408). The participants completed a survey which measured personality traits and the elements of TRA. Personality was assessed with Short Five and Short Dark Triad inventories. In addition, the participants read three scenarios where information security was at risk. After this they rated their probability to act in a similar way (intention) and their evaluation of the presented act (attitude). The scenarios in this study where divided in three groups according to their level of risk and each participant received scenarios only from a same level. The relationship between personality traits and responses in scenario situations was assessed with regression analysis. The measurement model was assessed with path analysis.

Results and conclusions. The measurement model fit the data when it was used to predict security attitudes and the harm presented in the scenarios was mild. The TRA structure was therefore found to predict attitudes in concrete situations as well. The relationship between personality traits and scenario responses was different for intentions and attitudes. Higher scores in two Dark Triad traits were linked to higher intentions. Higher extroversion predicted both lower intentions and attitudes. In addition, higher openness was linked to more positive attitudes, and these two connections remained in the measurement model. This study provided more information about the relationship between personality traits and information security behaviour and gave insight on which factors to improve to secure information in organisations.

Avainsanat – Nyckelord – Keywords
Information security behaviour, Theory of Reasoned Action, Big Five, Dark Triad, scenario method

Säilytyspaikka – Förvaringställe – Where deposited
Helsingin yliopiston kirjasto – Helda / E-thesis (opinnäytteet) *ethesis.helsinki.fi*

Muita tietoja – Övriga uppgifter – Additional information

Ihminen osana tietoturvaa: persoonallisuus ja perusteltu toiminta tietoturvakäyttäytymisen taustalla

Heini Marie Järviö
Pro gradu -tutkielma
Psykologia
Psykologian ja logopedian osasto
Helsingin yliopisto
Ohjaajat: Marjaana Lindeman & Petteri Simola

SISÄLLYSLUETTELO

1 JOHDANTO

Tietoturva on nykyihmisen elämässä arkipäiväinen elementti, joka tärkeydestään huolimatta saattaa jäädä liian vähälle huomiolle. Toukokuussa 2017 levinnyt Wannacry-virus levisi yli 230 000 tietokoneeseen 150 maassa, vahingoittaen lukuisien eri toimialojen yritysten toimintaa, sairaalat mukaan lukien (Ehrenfeld, 2017). Samalla se herätteli maailmaa tarkastelemaan tietoturvakäytänteitään huolellisemmin. Enenevästi lisääntyvä teknologian käyttö niin organisaatioissa kuin yksityiselämässä tarjoaakin yhteiskunnalle uudenlaisia mahdollisuuksia, mutta asettaa myös haasteita yksityisyydensuojan sekä luottamuksellisen tiedon suojaamiseen. Organisaatioissa voidaan tehdä erilaisia toimintasuunnitelmia turvallisuuden lisäämiseksi ja ne voivat vaihdella koulutuksista aina henkilöstövalintaan. Hyviä tietoturvakäytänteitä ja käyttäytymistä ovat esimerkiksi salasanojen säännöllinen vaihtaminen, varmuuskopioiden tekeminen ja virustorjuntaohjelmien käyttäminen (Shropshire, Warkentin & Sharma, 2015). Nämä koskevat organisaatioissa jokaista henkilöä, joilla on käyttöoikeus organisaation järjestelmiin ja/tai laitteisiin.

Tietoturvallisuuden ihmisnäkökulmalla tarkoitetaan yksityishenkilön tai organisaation jäsenen käsityksiä tietoturvan tärkeydestä, yksilön velvollisuuksista ja sopivasta turvallisuuden tasosta organisaatioon ja omiin toimiin suhteutettuna. On tutkittu, että jopa 35 % tietoturvaan liittyvistä virheistä on ihmisten aiheuttamia (Alaskar, Vodanovich & Shen, 2015). On siis perusteltua kiinnittää huomiota myös järjestelmien käyttäjiin itse tiedon suojaamisen lisäksi. Safa, Von Solms & Furnell (2016) käyttävätkin käsitettä kyberturvallisuus, kun halutaan puhua perinteisen tietoturvan komponenttien lisäksi ihmisen roolista tietoturvariskeissä – joko ihmisen toiminnan haavoittuvuudesta tai suorasta vaikuttamisesta tietoturvaan. Saadakseen mahdollisimman kokonaisvaltaisen kuvan ihmisen tietoturvakäyttäytymisestä organisaatiossa on otettava huomioon niin yksilö kuin ympäristö, jossa hän toimii. Tässä tutkimuksessa tarkoituksena onkin tarkastella, millaisia persoonallisuuteen ja organisaatioon liittyviä tekijöitä tietoturvakäyttäytymisen taustalla vaikuttaa.

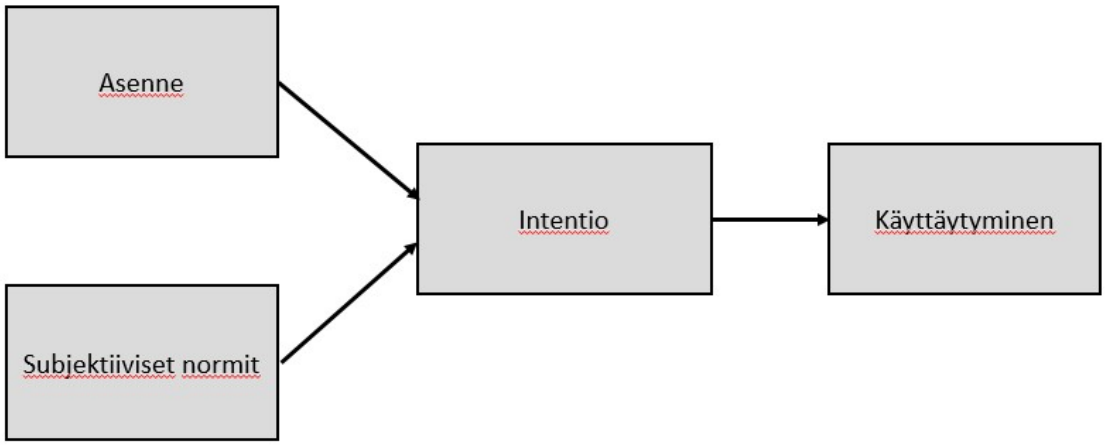
1.1 Perustellun toiminnan teoria ja tietoturvakäyttäytyminen

Tietoturvarikkeisiin johtavan käyttäytymisen tutkimus on lähivuosina ymmärrettävästi yleistynyt. Alaskarin ym. (2015) suhteellisen tuoreen katsauksen mukaan käytetyimpiä sosiaalipsykologisia teorioita tietoturvakäyttäytymisen selittäjinä ovat peloteteoria (*Deterrence*

Theory; Gibbs, 1975) suunnitelmallisen toiminnan teoria (*Theory of Planned Behaviour*, TPB; Ajzen, 1991) ja suojelumotivaatioteoria (*Protection Motivation Theory*; Rogers, 1975). Tietoturvakäyttäytymisen tutkimuksessa käytettyjen teorioiden kirjo on kuitenkin laaja, tuoreessa tutkimuksessaan Moody, Siponen ja Pahnila (2018) nimeävät jopa 11 teoriaa joita tietoturvakäyttäytymistä on pyritty ennustamaan. Peloteteoria, jonka juuret ovat kriminologiassa, pyrkii selittämään käyttäytymistä erilaisiin toimiin liittyvien rangaistusten ja hyötyjen punnitsemisen kautta (Achen ja Snidal, 1989). Teorian mukaan mahdollisten rangaistusten ollessa hyötyjä merkittävämpiä, ihminen päätyy vetäytymään toiminnasta. Peloteteoriaa on suosiostaan huolimatta kritisoitu tietoturvakäyttäytymisen tutkimuksessa siitä, että ihminen ei todellisuudessa ole niin rationaalinen kuin teoria antaa ymmärtää eikä se siten tavoita kaikkea tietoturvakäyttäytymisen taustalla vaikuttavaa. Rangaistuksiin liittyvien odotusten pienentämiseen voidaan käyttää esimerkiksi neutralisaatiota (Siponen & Vance, 2010). Neutralisaatiolla tarkoitetaan ajatusvääristymää, jonka kautta ihminen minimoi ajatuksen tasolla haitalliseen tekoon liittyviä väärinteon teemoja, saaden näin teon vaikuttamaan oikeutetummalta. Niin ikään suojelumotivaatioteoria (Rogers, 1975), joka alun perin kehitettiin tarkastelemaan terveyskäyttäytymistä, nojautuu yksilön arvioihin tietyn tapahtuman todennäköisyydestä, vakavuudesta ja sitä ehkäisevien toimien tehokkuudesta. Kumpikin näistä perustuu siis vahvasti siihen, että yksilö kykenee tekemään oikeellisia arvioita erilaisten toimien seurauksista ja suhteuttamaan nämä omaan toimintaansa. Valtaosa organisaation toimijoista on kuitenkin loppukäyttäjiä, eli niin sanottuja kuluttajia jotka ainoastaan käyttävät järjestelmiä, eivätkä millään tasolla hallinnoi tai kehitä niitä. He eivät ole erikoistuneet tietoturvaan ja -tekniikkaan ja on siksi perusteltua olettaa, että tietoturvaan liittyvien realististen arviointien tekeminen on valtaosalle organisaation jäsenistä haasteellista. Moniulotteisuudessaan tietoturvaan liittyvien riskien oton arviointi on myös haastavampaa kuin esimerkiksi rikollisuuden suhteen, minkä takia nämä teoriat eivät välttämättä parhaiten kuvaa arkipäiväistä tietoturvakäyttäytymiseen.

Tässä tutkimuksessa taustateoriana on käytetty Ajzeinin ja Fishbeinin (1975) perustellun toiminnan teoriaa (*Theory of Reasoned Action, TRA*), joka keskittyy pikemminkin tiettyä toimintaa kohti suuntaaviin tekijöihin kuin niistä poistyöntäviin. Teoriassa (kuva 1) keskeisenä käsitteenä on toiminnan aie eli intentio, jonka nähdään heijastelevan kyseisen toiminnan motivationaalisia tekijöitä silloin, kun toiminta on tahdonalaista. Aikeen voimakkuuden nähdään olevan suoraan verrannollinen toteutuvan toiminnan todennäköisyyteen. Teorian mukaan aietta puolestaan ennustavat asenne kyseistä toimintaa kohtaan sekä henkilökohtaiset normit.

Asenne määritellään teoriassa affektiiviseksi arvioksi teosta ja sen mahdollisista seurauksista. Subjektiivisilla normeilla puolestaan tarkoitetaan yksilön kokemusta siitä, mitä hänen lähipiirinsä ajattelisi toimesta, ja toisaalta halua toimia ympäristön odotusten mukaisesti. Perustellun toiminnan teorian mukaan ihminen toimii todennäköisimmin tietoturvan mukaisesti silloin, kun hän näkee tietoturvan myönteisessä valossa ja on sitoutunut ympäristöönsä, jossa niin ikään arvostetaan hyvää tietoturvatoimintaa. Ajzen (1991) laajensi perustellun toiminnan teoriaa myöhemmin suunnitelmallisen toiminnan teoriaksi (Theory of Planned Behaviour, TPB) lisäämällä siihen subjektiivisen kyvykkyyden tunteen kolmanneksi intention ennustajaksi. Subjektiivisella kyvykkyyden tunteella tarkoitetaan ihmisen omaa arviota kyvystään suorittaa jokin tietty toiminto, esimerkiksi selvitä jostakin tehtävästä. Se eroaa hallinnantunteesta olemalla tätä spesifimpi, ainoastaan yhteen toimintaan suuntautuva ja voi siten erota erilaisten toimintojen välillä. Esimerkiksi tietoturvan suhteen ihminen voi kokea korkeaa kyvykkyyttä pitää tietoturvaohjelmistot ajan tasalla, mutta heikkoa kyvykkyyttä omien tietojen suojaamisessa.



Kuva 1. Perustellun toiminnan teoria (Ajzen & Fishbein, 1975)

Sekä TRA että TPB on havaittu hyviksi intention ennustajiksi useissa eri yhteyksissä. Tässä tutkimuksessa taustateoriana päädyttiin käyttämään Ajzenin ja Fishbeinin (1975) teoriaa, jossa kyvykkyyden tunnetta ei tarkastella. Tämä on perusteltua, jotta tutkimusasetelma saatiin pidettyä yksinkertaisena. Vaikka TPB nähdään usein kehitellympänä ja siten parempana teoriana TRA:han verrattuna, aiemman tutkimuksen perusteella subjektiivisen kyvykkyyden tar-

kastelu ei ole välttämätöntä tai joissain yhteyksissä myöskään tarpeellista tietoturvakäyttäytymisen tutkimuksessa. Esimerkiksi Woonin ja Kankanhallin (2007) tutkimuksessa singaporelaisessa IT-asiantuntija-aineistossa TRA selitti suuremman osan intentiosta noudattaa tietoturvaohjeistuksia ohjelmistokehityksessä kuin TPB. Lisäksi heidän tutkimuksessaan subjektiivisella kyvykkyyden tunteella ei ollut lainkaan yhteyttä intentioon. Tämä lienee toisaalta selitettävissä tutkimuksen aineistolla, jolla koettu kyvykkyys oli todennäköisesti korkea ammattitaidosta johtuen. Koetun kyvykkyyden vähemmän merkittävää osuutta tietoturvaintentioiden ennustajana tukee kuitenkin myös Sommestadin ja Hallbergin (2013) katsaus 16 tietoturvakäyttäytymisen tutkimuksesta. Heidän yhteenvedossaan tarkasteltiin TPB:n mukaisia muuttujia tietoturvaintentioiden ennustajina, ja koetun kyvykkyyden havaittiin olevan keskimääräisesti hieman heikompi intention ennustaja verrattuna asenteisiin ja subjektiivisiin normeihin. Käyttäytymisen ennustajana se oli sen sijaan selkeästi heikompi kuin intentio. Toisaalta Changin (1998) tutkimuksessa, jossa näitä kahta teoriaa vertailtiin epäeettisen käyttäytymisen ennustajana, havaittiin että subjektiivinen kyvykkyys lisäsi selitysosuutta merkittävästi. Vaikuttaisi kuitenkin siltä, että TRA:n mukaiset tekijät selittänevät tarpeeksi tietoturvaintentioista ja koetun kyvykkyyden poisjättö on tutkimusteknisistä syistä johtuen perusteltua.

1.2 Tietoturvarikkeiden ja -rikkojien jaottelu

Tietoturvarikkeitä ja niiden tekijöitä voidaan jaotella erilaisin kriteerein, joiden lähtökohtana voi olla aikomus teon takana, tekijän roolin aktiivisuus rikkeen teossa tai käyttäjän suhde organisaatioon, jonka rike vaarantaa. Tässä tutkimuksessa fokus on niin sanotussa sisäpiiriteossa, jossa tietoturvauhan aiheuttaa organisaation sisäinen tai entinen jäsen. Pfleeger, Predd, Hunker ja Bulford (2010) määrittelevät tällaisen henkilön aiheuttaman sisäpiiriuhkan näin: ”sisäpiiriin kuuluvan henkilön teko, joka vaarantaa organisaation tiedot, järjestelmät tai resurssit vahingollisella tai epäsuotavalla tavalla” (s. 170). Sisäpiiritekijän vastakohta on organisaation ulkopuolinen tekijä, useimmiten hakkeri.

Sisäpiiriuhkan aiheuttavia henkilöitä voidaan jaotella teon intention mukaan. Rikkeen voidaan määritellä olevan kategorisesti tarkoituksellinen tai vahingossa tapahtuva. Tahaton tietovuoto voi tapahtua käyttäjän kokemattomuuden tai varomattomuuden seurauksena esimerkiksi tiedonkalastelun seurauksena. Tällaisten rikkeiden ehkäisemisessä voidaan hyödyntää koulutuksia, joissa käyttäjää voidaan auttaa kiinnittämään huomiota tietoturvaa vaarantaviin

toimiin. Tietoturvaintentioita voidaan tarkastella myös dimensionaalisesti. Esimerkki tästä on Guon, Yuanin, Archerin ja Connellyn (2011) käyttämä käsite aikeeton tietoturvarike. Tällä tarkoitetaan tekoa, joka tehdään tarkoituksenmukaisesti ja tietoisesti sääntöjä rikkoen, mutta ilman varsinaista pahantahtoista aietta. Tällainen aie voi olla ajan säästäminen työtehtävissä, johon yksilö voi pyrkiä esimerkiksi ohittamalla joitain tietoturvakäytänteitä. Vastakohtana aikeettomille ja vahingossa tapahtuville tietoturvarikkeille, tarkoituksellinen ja pahantahtoinen tietoturvarike tehdään päämääränä saavuttaa henkilökohtaista etua (esim. taloudellinen) tai pyrkimyksenä aiheuttaa organisaatiolle ongelmia (esim. vuotamalla luottamuksellista tietoa). Tarkoitukselliset tietoturvarikkeet ovatkin koulutusten ulottumattomissa, mutta organisaation ja yksilön taustalla vaikuttavat tietoturvakäyttäytymisen osatekijät voivat osoittautua hyödyllisiksi tuntea esimerkiksi riskien arviointia tehdessä. Alan tutkimuksen vähyydestä johtuen näitä tekijöitä ei kuitenkaan täysin tunneta vielä. Tässä tutkimuksessa päämääränä on selvittää, mitkä tietoturvakäyttäytymisen taustalla osatekijät olisi oleellista huomioida tietoturvan edistämisessä, erilaiset aikomukset huomioon ottaen. Tulos voi hyödyttää koulutusten suunnittelussa, ja mikäli yksilöllisiä eroja havaitaan, myös niiden kohdistamisessa erilaisille henkilöille. Yksilöinnin tukena käytetään persoonallisuuden piirteitä.

1.3 Käyttäjän persoonallisuus ja tietoturvakäyttäytyminen

Persoonallisuus on ihmisen suhteellisen pysyvä ominaisuus, joka vaikuttaa siihen, miten ihminen toimii ja on vuorovaikutuksessa. Pysyvyydestään johtuen sitä voidaankin hyödyntää ennustajana ihmisen toiminnalle erilaisissa tilanteissa, kun muut tilannetekijät tunnetaan. Vashisth ja Kumar (2013) kuvaavat artikkelissaan henkilökohtaisten piirteiden tarkastelua vahingollisen käyttäytymisen ennustajana termillä heikoimman lenkin lähestymistapa *(bad apple approach)*. Tarkastelun kohteena voi olla persoonallisuus, mutta myös esimerkiksi henkilön moraalinen kehitys. Persoonallisuuden tarkastelu tietoturvakäyttäytymisen ennustajana on toistaiseksi vähänlaisesti tutkittu asia. Selkeästi käytetyin persoonallisuuden piirreteoria tietoturvakäyttäytymisen tutkimuksessa on viiden suuren piirteen teoria (Big Five / Five Factor Model, McCrae ja Costa, 1987; Goldberg, 1990). Teoriassa persoonallisuus jaetaan viiteen dimensioon, jotka ovat tunnollisuus, avoimuus uusille kokemuksille, neuroottisuus, ekstroversio ja sovinnollisuus, sittemmin ystävällisyys. Eräässä aiemmassa kokeellisessa tutkimuksessa tarkasteltiin näitä piirteitä tietoturvaintention ja toteutuneen käyttäytymisen välistä yhteyttä muokkaavana tekijänä (Shropshire ym., 2015). Tunnollisuus ja sovinnollisuus vaikuttivat positiivisesti, kun tarkasteltiin, miten todennäköisesti tutkittavat toteuttivat aiettaan toimia

tietoturvakäytänteiden mukaisesti. Lisäksi persoonallisuus on yhdistetty myös asenteisiin, jotka johtavat aikomukseen tehdä tietovuoto (Maasberg, Warren & Beebe, 2015). Vaikuttaisi siis siltä, että persoonallisuuden tarkastelu tietoturvakäyttäytymisessä on sekä perusteltua että tärkeää.

Viiden suuren piirteen teoriaa on kuitenkin kritisoitu siitä, että se ei sisällä persoonallisuuden epärehellisiä ja pahantahtoisia elementtejä. Sittemmin onkin kehitelty uusia persoonallisuusteorioita, jotka pyrkivät kattamaan myös näitä niin sanottuja pimeitä piirteitä, kuten HEXACO (Lee & Ashton, 2004) ja Dark Triad (Paulhus & Williams, 2002). Ensin mainitussa viiteen piirteeseen on lisätty kuudes, rehellisyys-nöyryys-asteikko. Jälkimmäisellä puolestaan tarkastellaan subkliinisiä psykopatia-, narsismi- ja Machiavellismi-piirteitä. Käsitteellä subkliininen tarkoitetaan tilaa, jossa henkilöllä voi olla esimerkiksi narsistisia piirteitä, muttei vielä täytä narsistisen persoonallisuushäiriön diagnostisia kriteerejä. Psykologisten ongelmien tarkastelun jaottelu kliinisiin ja subkliinisiin ominaisuuksiin voidaankin ajatella käsittelevän psykologista problematiikkaa kategorisen sijaan dimensionaalisesti. Dark Triad -piirteiden sekä HEXACO-teorian kuudennen asteikon on sanottu olevan osittain päällekäisiä, ja rehellisyys-nöyryys -asteikko vaikuttaisikin mittaavan jonkinlaista Dark Triad -piirteiden jakamaa varianssia, niin sanottua pahuuden ydintä (Book, Visser & Volk, 2015).

Persoonallisuuden epärehellisten tai pahantahtoisten piirteiden tarkastelu tietoturvakäyttäytymisen tutkimuksessa on tärkeää, sillä sen voisi olettaa tavoittavan paremmin organisaatiolle vaarallisten, tahallisesti tehtyjen rikkomusten taustatekijöitä. Tutkimus tästä on kuitenkin vielä vähänlaista. Epärehellistä persoonallisuutta kuvaavat piirteet vaikuttaisivat ainakin jossain määrin ennustavan yleisesti epärehellistä käyttäytymistä työpaikalla (Deshong, Grant & Mullins-Sweatt, 2015; Scherer, Baysinger, Zolynsky & Lebreton, 2013). Tutkimusta niiden yhteydestä tietoturvakäyttäytymiseen ei kuitenkaan juurikaan ole. Tämän hetkisen tiedon perusteella pahantahtoisen persoonallisuuden voidaan siis arvella melko todennäköisesti vaikuttavan tietoturvakäyttäytymiseen, mutta tarkempi tieto näiden välisistä yhteyksistä on toistaiseksi hajanaista, mistä tämä tutkimus pyrkii tarjoamaan lisätietoa.

Organisaation työntekijöiden persoonallisuuden tarkastelu on perusteltua, sillä se voi osoittautua hyödylliseksi tietoturvarikkeiden ehkäisyssä. Kajzer, D'Arcy, Crowell, Striegel ja Van Bruggen (2014) tarkastelivat tutkimuksessaan viittä suurta piirrettä sekä Machiavellismia erilaisten tietoturvaviestien vaikuttavuuden ennustajina. Heidän tutkimuksessaan käytetyt viisi

eri viestityyppiä korostivat rangaistuksen uhkaa, moraalisuutta, katumusta, palautteen antamista ja kannustimia. He havaitsivat, että viisi suurta piirrettä olivat eri tavoin yhteydessä eri viestityyppeihin – esimerkiksi rangaistuksia korostavan viestin vaikuttavuus oli yhteydessä ainoastaan sovinnollisuuteen. Kannustimien suhteen niin ikään havaittiin yhteys ainoastaan avoimuuteen – ne vastaajat, jotka olivat avoimempia uusille kokemuksille, arvioivat kannustimiin viittaavat tietoturvaviestit vähemmän vaikuttaviksi. Palautetta korostavan viestin vaikuttavuus oli positiivisesti yhteydessä muihin viiteen suureen piirteeseen paitsi avoimuuteen, jonka yhteys oli negatiivinen. Sen sijaan Machiavellismilla ei havaittu yhteyttä minkään viestityypin vaikuttavuuden arvioon. Erilaisten persoonallisuuden piirteiden huomiointi esimerkiksi tietoturvaviestinnässä voi siis osoittautua hyödylliseksi esimerkiksi tietoturvaviestinnässä.

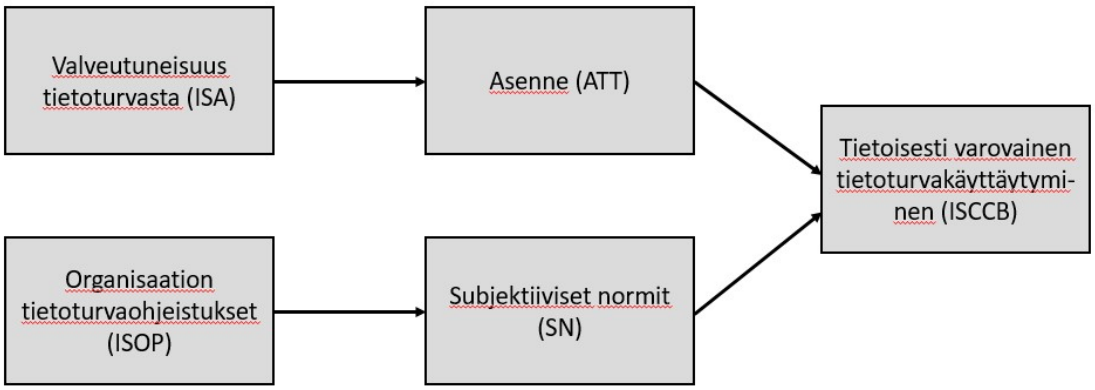
1.4 Organisaation tietoturvakulttuuri tietoturvakäyttäytymisen osatekijänä

Organisaation tietoturvakulttuurin voi vaikuttaa käyttäjän toimintaan esimerkiksi suuntaamalla tämän henkilökohtaisia arvoja samaan suuntaan. Ohjeistukset eivät itsessään muodosta kulttuuria, vaan myös se, miten niihin yleisesti suhtaudutaan. Esimerkiksi Guon, Yuanin, Archerin & Connellyn (2011) mukaan organisaation turvallisuuskulttuuria ennustaa sekä sen johtajien että työntekijöiden suhtautuminen tietoturvaan. Jos halutaan ennustaa yksilön tietoturvakäyttäytymistä, on siis tärkeää ottaa huomioon myös nämä asiat.

Organisaation tietoturvaohjeistuksien tulisi olla selkeitä ja ymmärrettäviä koherentin tietoturvakulttuurin luomiseksi (Safa ym., 2015). Safan ja kumppanien (2015) tutkimuksessa tarkasteltiin suunnitelmallisen toiminnan teoriaa (Ajzen, 1991) tietoisesti varovaisen tietoturvakäyttäytymisen ennustajana. Tietoisesti varovaisen tietoturvakäyttäytymisen *(Information Security Conscious Care Behaviour, ISCCB*) nähtiin tässä heijastelevan intentiota toimia hyvän tietoturvakäytänteen mukaisesti. Heidän tutkimuksessaan tarkasteltiin myös kolmea muuta tekijää, joiden ajateltiin vaikuttavan suunnitelmallisen toiminnan teorian pääkomponentteihin. Valveutuneisuuden tietoturvasta nähtiin olevan yhteydessä tietoturva-asenteisiin, organisaation tietoturvaohjeistusten subjektiivisiin ja normeihin ja kokeneisuuden koettuun kyvykkyyteen. Mallin sopivuutta tarkasteltiin malesialaisessa tietoturva-asiantuntija-aineistossa, jossa osallistujat vastasivat näitä osa-alueita koskeviin osioihin kyselylomakkeella. Lopullisessa mallissa teorian kaikki osatekijät olivat yhteydessä siihen, miten harkitsevasti vastaaja

koki toimivansa tietoturvan suhteen. Heidän tuloksensa mukaisesti intentioita toimia tietoturvallisesti voitaisiin siis edistää vahvistamalla subjektiivisia normeja tietoturvaohjeistusten kautta, sekä vaikuttamalla tietoturva-asenteisiin lisäämällä valveutuneisuutta.

Tässä tutkimuksessa tarkoituksena on mukailla Safan ym. (2015) tutkimuksen TRA:n mukaisia osioita ja niiden taustatekijöitä kuvan 2 mukaisesti. Heidän tutkimuksessaan ei kuitenkaan tarkasteltu todellista käyttäytymistä, jota lähemmäs tällä tutkimuksella pyritään pääsemään skenaarioasetelmaa hyödyntäen. Tämä tehdään yhdistämällä kuvan 2 mukainen rakenne kuvitteellisessa tilanteessa tarkasteltuun tietoturvaintentioon ja -asenteeseen.



Kuva 2. Safan ym., (2015) tutkimuksen mukainen rakenne harkitsevaan tietoturvakäyttäytymiseen johtavista tekijöistä.

Vashisthin & Kumarin (2013) aiemmin kuvatun, heikoimman lenkin lähestymistavan vastakohta on heikoimman ketjun lähestymistapa, *bad barrel approach*, jonka mukaan organisaatio ja sen kulttuuri itsessään ratkaisevat, miten yksittäinen henkilö päättää käyttäytyä. Kuitenkin, kuten Funder (2006) tiivistää, toteutunut käyttäytyminen on seurausta ennemminkin persoonallisuuden ja tilannetekijöiden yhtälöstä. Aiemmassa tutkimuksessa on esimerkiksi havaittu, että epärehellinen persoonallisuus vaikuttaisi kasvattavan henkilön todennäköisyyttä syyllistyä vahingolliseen työkäyttäytymiseen organisaatioissa, joiden kulttuuri on sallivampaa (Wiltshire, Bourdage & Lee, 2014). Siksi tietoturvakäyttäytymisen tutkimuksessa voikin olla hyödyllisintä tarkastella tietoturvakäyttäytymistä kummastakin lähestymistavasta. Persoonal-

lisuus ja organisaation kulttuuri voivat siis tarjota perustan, jolla toteutuvaa tietoturvakäyttäytymistä voidaan ennustaa. Tämän tutkimuksen pyrkimyksenä onkin tarkastella, minkälaisia yksilöön ja organisaatioon liittyviä tekijöitä tietoturvakäyttäytymisen taustalla voidaan havaita.

1.5 Hypoteesit

Tämän tutkimuksen pyrkimyksenä on täyttää aiemman tutkimuksen puutteita persoonallisuuden, organisaation tietoturvakulttuurin sekä näiden yhdistelmän yhteydestä yksilön tietoturvakäyttäytymiseen. Koska persoonallisuuden tutkimus tietoturvakäyttäytymisen ennustajana on painottunut viiden suuren piirteen tarkasteluun, tässä tutkimuksessa päämääränä on tarkastella, voisiko myös epärehellistä persoonallisuutta tarkastelevista inventaareista, kuten Short Dark Triad, olla hyötyä tietoturvarikkeiden riskitekijöiden kartoituksessa. Itsearvioidun käyttäytymisen lisäksi tietoturvakäyttäytymistä tutkitaan skenaarioasetelman avulla, jossa tavoitteena on päästä hieman lähemmäs oikeaa käyttäytymistä. Skenaarioasetelmassa vastaajat saavat luettavakseen hypoteettisia tietoturvan vaarantavia tilanteita, joiden jälkeen he arvioivat suhtautumistaan tähän kuvaukseen. Itsearviointikyselyiden vaarana on vastausten kaunistelu sosiaalisesti suotavampaan suuntaan, mikä erityisesti haitallista käyttäytymistä tarkastellessa saattaa vääristää tuloksia. Skenaarioiden käyttäminen onkin suhteellisen yleistä epäeettistä käyttäytymistä tarkastelevissa tutkimusasetelmissa ja enenevissä määrin yleistymässä myös tietoturvakäyttäytymisen tutkimuksessa (Vance, Siponen & Pahnila, 2012).

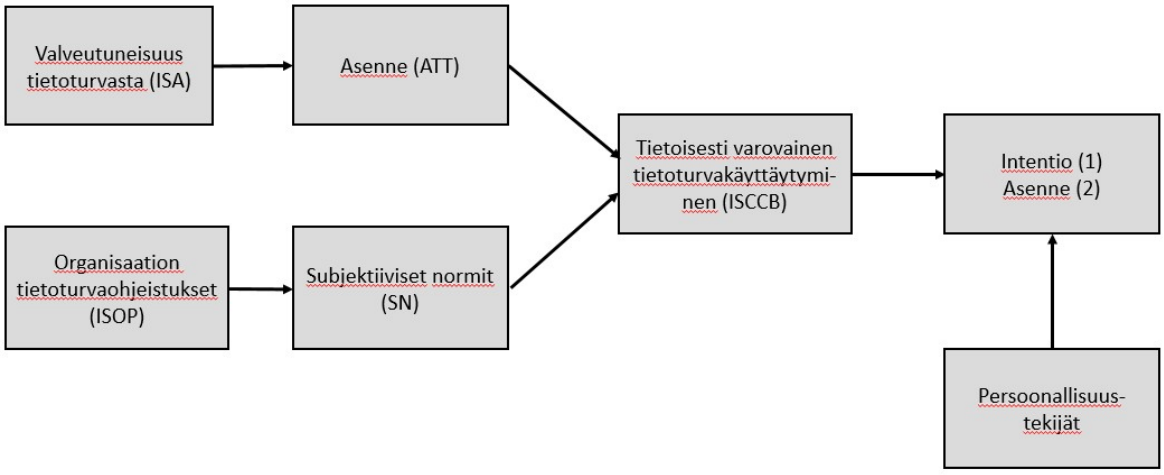
Näin ollen, tämän tutkimuksen päämääränä on tarkastella, toteutuuko aineistossa kuvassa 3 esitetty mittausmalli. Tähän tutkimuskysymykseen liittyen asetetaan hypoteesit:

1. Tietoturvavalveutuneisuuden, organisaation tietoturvaohjeistuksien, yksilön tietoturva-asenteiden ja subjektiivisten normien yhteys harkitsevaan tietoturvakäyttäytymiseen on positiivinen.
2. Harkitsevuus tietoturvakäyttäytymisessä on negatiivisesti yhteydessä arvioituun todennäköisyyteen toimia skenaariossa kuvatulla tavalla sekä tekoon kohdistuvaan asenteeseen.

3a. Arvioitu todennäköisyys toimia skenaarion kuvaamalla tavalla on pienempi niissä tilanteissa, joiden vaarallisuusaste tietoturvalle on vakava, kuin niissä joissa vaarallisuusaste on vain lievä.

3b. Arvioitu asenne skenaarion kuvaamaa tekoa kohtaan on myönteisempi niissä tilanteissa, joiden vaarallisuusaste tietoturvalle on lievä, kuin niissä joissa vaarallisuusaste on vakavampi.

4. Persoonallisuuden piirteet ovat yhteydessä arvioituun todennäköisyyteen toimia skenaariossa kuvatulla tavalla sekä siihen kohdistuvaan asenteeseen
    a. Tunnollisuuden ja sovinnollisuuden suhteen yhteys on negatiivinen
    b. Machiavellismin, narsismin ja psykopatian suhteen yhteys on positiivinen



Kuva 3. Tutkimuksen mittausmalli

2 MENETELMÄT

2.1. Osallistujat

Tutkimuksen aineisto (n=408) koostui Maanpuolustuskorkeakoulun ensimmäisen vuoden sekä Helsingin yliopiston opiskelijoista. Vastaajien iän keskiarvo oli vastaushetkellä 24.4 vuotta (kh = 5.67) ja heistä 50.7 % oli naisia, 47.5 % miehiä ja 1.7 % kertoi sukupuolekseen ”muu”. Suurimmalla osalla vastaajista (65.4 %) korkein koulutus oli ylioppilastutkinto, 3.4 %:lla puolestaan ammatillinen tutkinto, 23.5 %:lla alempi korkeakoulututkinto ja 7.5 %:lla ylempi korkeakoulututkinto tai tohtorikoulutus.

Helsingin yliopistolta kerätyn aineiston (n = 259) keruu toteutettiin marraskuun 2016 ja tammikuun 2017 välisenä aikana rekrytoimalla vastaajia opiskelijajärjestöjen sähköpostilistojen kautta. Vastausten keruu toteutettiin e-lomake-järjestelmässä. Maanpuolustuskorkeakoulun aineiston (n = 149) keruu tehtiin lokakuussa 2016 maanpuolustuskorkeakoulun tiloissa Santahaminassa.

Erilaisista aineistonkeruumenetelmistä johtuen puuttuvia arvoja oli ainoastaan Maanpuolustuskorkeakoulusta kerätyssä otoksessa. Kaiken kaikkiaan puuttuvia arvoja oli yhteensä 52 vastaajalla. Jatkotarkasteluihin valittiin ne vastaajat, jotka olivat vastanneet vähintään 80 %:iin kaikista tarvittavista osioista tai yksittäisen asteikon osioista. Näin jatkotarkasteluista poistettuja vastaajia oli yhteensä 6. Koska puolelta näistä vastaajista puuttuivat myös taustamuuttujiin liittyvät tiedot, ei aineistossa pystytty tekemään katoanalyysiä.

Lähes kaikki vastaajat ilmoittivat käyttävänsä tietokonetta ja kaikki käyttivät internetiä. Puolet vastaajista ilmoitti käyttävänsä aktiivisesti kahta tai kolmea sosiaalisen median palvelua, ja kaikista vastaajista vastaosa käytti näitä palveluja pääasiassa muiden julkaisujen seuraamiseen. Pankkiasiat hoidettiin pääosin omilla laitteilla – 71,8 % omalla tietokoneella ja 26,5 % omalla mobiililaitteella. Vertaisverkkoa ilmoitti käyttävänsä 28,7 % vastaajista. Tietoturva oli aineiston vastaajilla pääosin kunnossa – 68 % ilmoitti, että tietokoneessa on ajantasainen virusturva. Sen sijaan 15,5 %:lta virustorjunta puuttui tai se ei ollut ajan tasalla. Väliaikaiset internet-tiedostot ja selaushistoria olivat vastaajille tuttuja – ainoastaan yksi vastaaja ilmoitti, ettei tiedä mitä ne ovat. Tästä huolimatta vain 35,5 % kertoi poistavansa kyseiset tiedot aina julkista tietokonetta käyttäessään, 14 % ei koskaan.

2.2. Arviointimenetelmät

Persoonallisuus

Viittä suurta persoonallisuuspiirrettä (avoimuus uusille kokemuksille, neuroottisuus, sovinnollisuus, tunnollisuus ja ekstroversio) mitattiin Short Five -kyselyllä (Konstabel, Lönnqvist, Walkowitz, Konstabel & Verkasalo, 2012). Kysely koostuu 65 väittämästä (esim. ” Olen usein hermostunut, tunnen levottomuutta ja pelkoa sekä olen huolissani siitä, että asiat voivat mennä vikaan”), joiden sopivuutta itseensä vastaaja arvioi seitsemänportaisella asteikolla (1 = täysin eri mieltä – 7 = täysin samaa mieltä). Kutakin viittä piirrettä tutkittiin 13 väittämällä. Lyhyem-

män inventaarin käyttöön päädyttiin pyrkimyksenä pitää kokonaiskyselyn pituus sopivana. Kyselyn rakenteen on aiemmin todettu noudattavan NEO-PI-R-inventaarin mukaista rakennetta suomalaisessa populaatiossa (Konstabel ym., 2012).

Subkliinistä psykopatiaa, narsismia ja Machiavellismia tutkittiin Short Dark Triad -inventaarilla (Jones & Paulhus, 2014). Inventaari koostuu 27 väittämästä (esim. ” On hyvä saada merkittäviä ihmisiä omalle puolelle keinoja kaihtamatta”), joiden sopivuutta itseensä vastaajat arvioivat viisiportaisella asteikolla (1 = täysin eri mieltä – 5 = täysin samaa mieltä). Kutakin kolmea Dark Triad -teorian mukaista piirrettä tutkittiin yhdeksällä väittämällä. Lyhennettyyn inventaariin päädyttiin tavoitteena pitää kokonaiskyselyn pituus sopivana. Inventaarin englanninkielisen alkuperäisversion on osoitettu olevan tarkkuudeltaan yhtä hyvä kuin sekä perinteisempien subkliinisiä piirteitä tarkastelevien inventaarien että lähiomaisten arvion (Jones & Paulhus, 2014).

Koska Short Dark Triad -inventaarista ei ole tehty suomenkielistä versiota, sen osiot suomennettiin ensin. Kaikki suomenkieliset osiot ja niiden keskiarvot sekä keskihajonnat on esitetty liitteessä 1. Suomennetun inventaarin rakenteen tarkasteluksi suoritettiin faktorianalyysi. Normaalijakaumaoletus ei täyttynyt useamman muuttujan kohdalla, mitä pyrittiin korjaamaan neliöjuuri- ja logaritmimuunnoksilla. Tämä ei kuitenkaan tuottanut merkittävää muutosta muuttujien jakaumille, mitä faktorianalyysissä korjattiin robustilla huber white -korjauksella. Aineisto ei noudattanut Jonesin ja Paulhuksen alkuperäistutkimuksen mukaista rakennetta konfirmatorisessa faktorianalyysissä (RMSEA = .083(.078;.088), TLI = .604). Niin ikään eksploratiivisessa faktorianalyysissä ei kyetty löytämään alkuperäistutkimuksen mukaista ratkaisua, mikä saattaa olla seurausta aineiston valikoituneisuudesta. Myös inventaarin suomentaminen on saattanut vaikuttaa osioiden tulkintaan niin, että ne eivät ole käsitettävissä täysin identtisesti kuin alkuperäisversiossa. Lisäksi kolmen piirteen erillisyyttä on kritisoitu, ja on ehdotettu, että ne olisi tiivistettävissä yhdeksi piirteeksi. Koska Dark Triad -inventaarin rakenne on kuitenkin aiemmassa tutkimuksessa saanut tukea, sen käyttöä päädyttiin jatkamaan tässäkin tutkimuksessa.

Lopulliset kolme Dark Triad -muuttujaa muodostettiin Jonesin ja Paulhuksen (2014) alkuperäistutkimusta mukaillen laskemalla keskiarvot kutakin kolmea vastaavista seitsemästä osioista. Kunkin Dark Triad -piirremuuttujan reliabiliteetti (Cronbachin α) oli hyväksyttävä, Machiavellismille (.75), psykopatialle (.63) ja narsismille (.75).

Tietoturvakäyttäytyminen

Tietoturvakäyttäytymisen taustalla vaikuttavien tekijöiden tutkimuksessa käytettiin Safan ym., (2015) tutkimukseen kehiteltyjä perustellun toiminnan teorian mukaisia muuttujia sekä samaisessa tutkimuksessa havaittua rakennetta, jossa tietoisesti varovaisen tietoturvakäyttäytymisen taustalla on neljän muun muuttujan rakenne (kuva 2). Vastaajat arvioivat yksimielisyyttään väittämien (esim. ” Oppilaitoksessani arvostetaan tietoturvaohjeistuksien ja -käytäntöjen mukaan toimimista”) kanssa viisiportaisella asteikolla (1 = täysin eri mieltä – 5 = täysin samaa mieltä). Esitetyt väittämät liittyivät tietoturva-asenteisiin (5 kpl), organisaation tietoturvaohjeistuksiin (4 kpl), subjektiivisiin normeihin (4 kpl), tietoturvavalveutuneisuuteen (4 kpl) ja tietotoisesti varovaiseen tietoturvakäyttäytymiseen (5 kpl). Inventaarin kaikki osiot on esitetty liitteessä 1.

Osa muuttujista noudatti vasemmalle vinoa jakaumaa, mitä pyrittiin korjaamaan muuttujamuunnoksilla. Tämä ei tuottanut merkittävää eroa muuttujien jakaumissa, joten jatkotarkasteluissa päädyttiin käyttämään alkuperäisiä muuttujia. Suomennetun inventaarin rakenteen tutkimiseksi suoritettiin konfirmatorinen faktorianalyysi huber white -korjauksella (esim. Hox, Maas & Brinkhuis, 2010) jakaumien normaalisuusoletuksen rikkoutumisen takia. Aineistossa ei toteutunut Safan ym., (2015) alkuperäistutkimuksen mukainen rakenne (RMSEA = .07 (0.06;0.077), TLI = .84). Rakennetta tarkasteltiin kuitenkin vielä eksploratiivisella viiden faktorin faktorianalyysillä, jonka yhteensopivuus oli hyvä (RMSEA = 0.055 (0.045;0.062), TLI = 0.913). Ratkaisu rotatoitiin oblimin-rotaatiolla, koska taustalla oletettavan rakenteen mukaisesti muuttujien voidaan olettaa korreloivan keskenään. Näin saatu faktorirakenne (taulukko 1) vastasi kohtuullisen hyvin alkuperäistutkimuksen mukaista rakennetta. Faktorit F1, F2, F3 ja F4 nimettiin niille latautuvien muuttujien mukaisesti valveutuneisuudeksi tietoturvasta (ISA), organisaation tietoturvaohjeistuksiksi (ISOP), tietoiseksi varovaisuudeksi (ISCCB) ja asenteeksi tietoturvaa kohtaan (ATT). Cronbachin alfa -reliabiliteettikertoimet näille faktoreille olivat (.79), (.79), (.69) ja (.70). Koska subjektiiviset normit (SN) -osiot jakaantuivat eri faktoreille ja kokonaisuus oli reliabiliteetiltaan heikko (Cronbachin $\alpha = .44$), päädyttiin jatkotarkasteluissa käyttämään ainoastaan SN2-osiota, koska sen nähtiin parhaiten heijastavan asteikon taustalla olevaa teoreettista ajatusta. Muut neljä muuttujaa muodostettiin laskemalla keskiarvo kunkin vastaavista osioista. Inventaarin kaikkien osioiden keskiarvot ja -hajonnat on esitetty liitteessä 1.

Taulukko 1. Tietoturvakäyttäytymisasteikon osioiden latautuminen faktoreille. Voimakkuudeltaan 0.3 tai tätä suuremmat lataukset faktoreille on esitetty tummennettuina.

	F1	F2	F3	F4	F5
ISCCB1	0.09	-0.04	**0.59**	0.06	-0.14
ISCCB2	-0.01	0.12	**0.41**	-0.06	-0.04
ISCCB3	-0.02	0.09	**0.70**	0.09	-0.03
ISCCB4	0.10	-0.04	**0.32**	0.28	0.02
ISCCB5	0.23	-0.05	0.22	0.23	0.06
ISOP1	0.06	**0.60**	0.19	-0.06	0.05
ISOP2	0.18	0.12	**0.49**	0.07	0.16
ISOP3	**0.38**	0.22	0.18	-0.04	0.03
ISOP4	-0.02	**0.95**	-0.05	0.07	-0.03
ATT1	-0.01	-0.08	**0.36**	**0.39**	0.02
ATT2	0.10	0.25	0.09	0.14	0.10
ATT3	0.15	0.22	-0.01	**0.56**	-0.02
ATT4	-0.06	0.01	0.04	**0.68**	-0.02
ATT5	0.15	0.08	0.12	**0.50**	0.06
SN1	-0.09	0.01	0.00	0.07	**0.58**
SN2	0.07	**0.36**	**0.31**	-0.05	0.28
SN3	0.00	-0.08	-0.11	-0.06	**0.61**
SN4	0.17	**0.46**	0.14	-0.07	0.00
ISA1	**0.79**	-0.02	-0.03	0.11	-0.03
ISA2	**0.56**	0.06	-0.01	-0.19	-0.01
ISA3	**0.85**	0.00	-0.04	0.04	0.01
ISA4	**0.62**	0.04	0.21	-0.09	-0.06

ISCCB = tietoisesti varovainen tietoturvakäyttäytyminen, ISOP = organisaation tietoturvaohjeistukset, ATT = asenne tietoturvaa kohtaan, SN = subjektiiviset normit, ISA = valveutuneisuus tietoturvasta.

Skenaariot

Tietoturvakäyttäytymistä tarkasteltiin myös skenaarioasetelmalla, pyrkimyksenä on päästä lähemmäs todellista käyttäytymistä kuin mitä pelkällä väittämiin perustuvalla kyselylomakkeella on mahdollista. Kukin vastaajista sai lomakkeessa luettavakseen kolme hypoteettista tilannetta eli skenaariota, joissa tietoturva vaarantuu eriasteisesti. Yhteensä tutkimuksessa käytettiin yhdeksää erilaista skenaariota, jotka oli jaoteltu tilanteen vaarallisuusasteen mukaisesti kolmeen ryhmään: lievä haitta, kohtuullinen haitta ja korkea haitta tietoturvalle. Tutkimuksen osallistujat jaettiin kolmeen ryhmään siten, että kukin sai luettavakseen kolme saman vaarallisuusasteen mukaista skenaariota. Skenaarioiden esitysjärjestys oli satunnaistettu vastaajien kesken.

Skenaariotilanteet muodostettiin Siposen ja Vancen (2010) tutkimuksen skenaariotilanteita tämän tutkimuksen vastaajapopulaatioon sovittaen. Lisäksi kehiteltiin uusia tilanteita, jotta tietoturvakäyttäytymistä saatiin kartoitettua mahdollisimman laajassa valikoimassa erilaisia arkipäivän tilanteita. Skenaariot pyrittiin muodostamaan korkeakouluympäristöön sopiviksi, jotta ne koettaisiin mahdollisimman realistisiksi vastaajien näkökulmasta. Tutkimukseen päätyneet skenaariot valittiin laajemmasta kokoelmasta kehiteltyjä skenaarioita, joiden sopivuutta tutkimukseen arvioitiin pilottitutkimuksessa. Pilottitutkimuksessa vastaajat (n=20) lukivat yhteensä 16 kehiteltyä skenaariotilannetta ja arvioivat tilanteiden uskottavuutta ja ymmärrettävyyttä viisiportaisella asteikolla sekä luokittelivat tilanteen mielestään sopivimpaan kolmesta edellä mainitusta vaarallisuusluokasta. Lopulliseen tutkimukseen valikoituneet skenaariot olivat arvioidulta vaarallisuusasteeltaan luokkien sisällä yhdenmukaisia ja arvioitiin realistisiksi sekä ymmärrettäviksi. Kaikki lopulliset yhdeksän skenaariota esitetty liitteessä 2.

Esimerkki skenaariotilanteesta:

Mikael on juuri aloittanut yliopiston, ja hänen täytyy keksiä salasana yliopiston intranet-käyttäjätunnusta varten. Hän luo salasanakseen “Mikael1”. Toisena opiskeluvuonna, kun järjestelmä pyytää häntä vaihtamaan salasanansa, Mikael valitsee salasanakseen “Mikael2”. Kolmantena opiskeluvuotena järjestelmä pyytää jälleen vaihtamaan salasanan, jolloin Mikael vaihtaa salasanakseen “Mikael3”.

Tämän tutkimuksen kyselylomakkeessa skenaarioiden esittämisen jälkeen vastaajille esitettiin tilanteeseen liittyviä väittämiä, joissa kartoitettiin heidän arviotaan tilanteesta (asenne) sekä todennäköisyyttä toimia tilanteessa kuvatulla tavalla (intentio). Skenaarioihin liittyvät osiot oli muodostettu mukailemalla Guon ym. (2011) skenaariotutkimuksessaan käyttämiä kysymyksiä ja tätä tutkimusta varten osiot suomennettiin. Tässä tutkimuksessa tarkastelun kohteena ovat intentiota (2 kpl) ja asennetta (6 kpl) skenaariotilanteessa tarkastelevat osiot (taulukko 2). Intentio-osioissa (esim. ”Toimisin skenaarion kuvaamalla tavalla, jos olisin kyseinen ihminen”) vastaajat arvioivat todennäköisyyttään toimia tilanteessa kuvatulla tavalla viisiportaisella asteikolla (1 = täysin eri mieltä – 5 = täysin samaa mieltä). Asenneosioissa vastaaja arvioi suhtautumistaan kuvattuun tekoon viisiportaisella asteikolla, jonka ääripäät oli määritelty kysymyskohtaisesti (taulukko 2).

Taulukko 2. Skenaariotilanteissa esitetyt intentio- ja asenneosiot

Intentio	
Intentio1	Toimisin skenaarion kuvaamalla tavalla, jos olisin kyseinen ihminen.
Intentio2	Toimisin skenaarion kuvaamalla tavalla, jos olisin samankaltaisessa tilanteessa.
Asenne	
Asenne1	Jos toimisin näin se olisi huono … hyvä idea
Asenne2	Jos toimisin näin se olisi haitallista … hyödyllistä
Asenne3	Jos toimisin näin se olisi väärin … oikein
Asenne4	Jos toimisin näin se olisi epäeettistä … eettistä
Asenne5	Jos toimisin näin se olisi arvotonta … arvokasta
Asenne6	Jos toimisin näin se olisi laitonta … laillista

Koska kukin vastaaja sai luettavakseen kolme skenaariota, saatiin kultakin vastaajalta siis kolme vastausta jokaiseen intentio- ja asenneosioon. Keskimääräisen vastaamisen selvittämiseksi näistä kolmesta vastauksesta laskettiin keskiarvo. Tämän jälkeen kullekin osallistujalle muodostettiin keskimääräiset intentio- ja asennemuuttujat laskemalla keskiarvo intentio-

ja asennemuuttujista. Reliabiliteetti (Cronbachin α) näin muodostetulle intentiomuuttujalle oli korkea (.91) ja asennemuuttujalle hieman voimakkaampi (.93). Lopulliset muuttujat olivat jakaumaltaan oikealle vinoja, mitä korjattiin tekemällä niille logaritmimuunnos.

2.3 Tilastolliset menetelmät

Faktorianalyysit, polkuanalyysi ja niihin liittyvät taustatarkastelut suoritettiin R-ohjelmiston versiolla 1.01.143. Tarkasteluihin käytettiin paketteja psych (Rewelle, 2015, versio 1.7.8) ja lavaan (Rosseel, 2012, versio 0.5-23.1097). Kaikki muut tarkastelut ja muuttujamuunnokset tehtiin SPSS-ohjelmiston versiolla 23.0.0.0.

3 TULOKSET

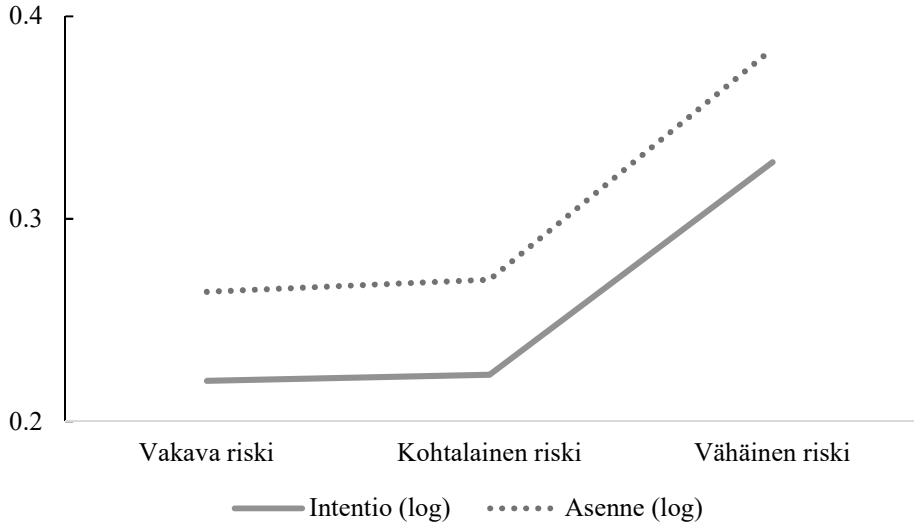
3.1 Skenaarion vakavuusasteen yhteys asenteisiin ja intentioihin

Taulukossa 3. on esitetty muuttujien tarkasteluissa käytettyjen muuttujien väliset korrelaatiot sekä keskiarvot ja -hajonnat. Skenaarioiden yhteydessä vastaajat arvioivat todennäköisyyttään syyllistyä kuvattuun tekoon sekä asennettaan sitä kohtaan. Yksisuuntaisella varianssianalyysillä tutkittiin, oliko esitetyn tilanteen vakavuusasteen suhteen eroa näissä arvioissa, jotta saatiin selville, oliko aineistoa tarve ryhmitellä vakavuuden mukaan jatkotarkasteluissa. Skenaarion vakavuusasteella oli merkitsevä päävaikutus sekä intention ($F(2,405) = 17.83$, $p < .001$) että asenteen suhteen ($F(2,405) = 46.27$, $p < .001$). Sekä asenne- että intentiomuuttuja saivat korkeampia arvoja vähäisen riskin ryhmässä kuin kahdessa muussa ($p < .001$). Sen sijaan kohtalaisen ja vakavan riskin ryhmien välillä näissä muuttujissa eroa oli vain hyvin vähän (kuva 4). Tästä johtuen skenaarioryhmät 1 ja 2 yhdistettiin vaarallisemman riskin ryhmäksi, jota jatkotarkasteluissa verrattiin ryhmään 3 (vähäinen riski).

Taulukko 3. Tutkimuksessa käytettyjen muuttujien tunnusluvut ja korrelaatiot.

		ka	Kh	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Int (ske)	0.26	0.18	1														
2	Att (ske)	0.31	0.13	0.53**	1													
3	N	-9.59	11.35	0.24**	0.17**	1												
4	E	10.1	8.82	-0.13*	-0.16**	-0.24**	1											
5	O	12.5	9.15	0	0.12*	0.33**	0.26**	1										
6	A	13.8	7.69	-0.18**	-0.10*	-0.10*	0.25**	0.44**	1									
7	C	11	10.9	-0.30**	-0.21**	-0.78**	0.31**	-0.21**	0.38**	1								
8	Mach	2.33	0.60	0.13*	0.1	0.08	-0.23**	-0.28**	-0.52**	-0.13*	1							
9	Na	2.73	0.68	0.01	-0.06	-0.38**	0.45**	-0.17**	-0.09	0.39**	0.21**	1						
10	Psyk	1.93	0.53	0.19**	0.07	-0.02	0.04	-0.29**	-0.48**	-0.09	0.50**	0.39**	1					
11	ATT	4.29	0.50	-0.26**	-0.18**	-0.33**	0.19**	0.03	0.18**	0.34**	-0.1	0.12*	-0.06	1				
12	ISA	3.61	0.85	-0.27**	-.24**	-0.48**	0.11*	-0.18**	0.03	0.40**	0.04	0.22**	0.15*	0.38**	1			
13	ISCCB	3.75	0.64	-0.26**	-0.20**	-0.39**	0.16**	-0.10*	0.17**	0.43**	-0.03	0.18**	0.02	0.57**	0.49**	1		
14	ISOP	3.96	0.77	-0.26**	-0.22**	-0.55**	0.19**	-0.19**	0.17**	0.53**	-0.06	0.27**	0.08	0.55**	0.59**	0.59**	1	
15	SN2	3.63	1.16	-0.18**	-0.17**	-0.47**	0.06	-0.26**	0.08	0.45**	-0.04	0.22**	0.06	0.38**	0.36**	0.43**	0.62**	1

** p < .05, ** p < .001, Int (ske) = intentio skenaariotilanteessa, logaritmimuunnettu, Att (ske) = asenne skenaariotilanteessa, logaritmimuunnettu, N = neuroottisuus, E = ekstroversio, O = avoimuus uusille kokemuksille, A = sovinnollisuus, C = tunnollisuus, Mach = Machiavellismi, Na = narsismi, Psyk = psykopatia, ATT = asenne tietoturvaa kohtaan, ISA = tietoturvavalveutuneisuus, ISCCB = tietoinen varovaisuus tietoturvassa, ISOP = organisaation tietoturvaohjeistukset, SN = SN2, ”Oppilaitokseni tietoturvakulttuuri vaikuttaa toimintaani”*



Kuva 4. Logaritmimuunnettujen asenne- ja intentiomuuttujien keskiarvot kolmessa skenaario-ryhmässä.

3.2 Persoonallisuuspiirteiden yhteys tietoturvakäyttäytymiseen

Regressioanalyysillä kartoitettiin mitä persoonallisuustekijöitä olisi syytä huomioida jatkotarkasteluissa tutkimuksen mittausmallissa (kuva 2). Logaritmimuunnettuja intentio- ja asennemuuttujia ennustettiin regressioanalyysissä viidellä suurella ja Dark Triad -persoonallisuuspiirteillä (taulukko 4). Intention suhteen vahvimmat ennustajat olivat tunnollisuus ($\beta = -.30$) sekä narsismi ($\beta = .15$) ja psykopatia ($\beta = .15$). Malli oli merkitsevä ($F(8,392) = 8.65$, $p < .001$, $R^2 = .15$). Asenteen suhteen merkitseviä selittäjiä olivat ekstroversio ($\beta = -.19$) ja avoimuus ($\beta = .19$). Tämäkin malli oli merkitsevä ($F(8,392) = 6.10$, $p < .001$, $R^2 = .11$). Kaikki merkitsevät persoonallisuusmuuttujat otettiin jatkotarkasteluihin. Tunnollisuuden suhteen toleranssiarvo oli alle 0.3, jota pidetään kriittisenä rajana jatkotarkasteluiden kannalta. Koska muista ennustajista niin pientä osaa käytettiin jatkotarkasteluissa, tätä ei kuitenkaan pidetty ongelmana.

Taulukko 4. Regressioanalyysi, jossa persoonallisuuspiirteillä ennustettiin logaritmi-muunnettuja skenaariotilanteen intentio- ja asennemuuttujia. Tilastollisesti merkitsevät yhteydet on esitetty tummennettuna

	Intentio			Asenne			
	β	t	p	β	t	p	Toleranssi
Neuroottisuus	.06	.73	.47	.02	.23	.821	.33
Ekstroversio	-.12	-2.04	**.04**	-.19	-3.04	**.003**	.58
Avoimuus	.01	.21	.84	.19	3.00	**.003**	.56
Sovinnollisuus	.03	.40	.69	-.05	-.71	.48	.41
Tunnollisuus	-.30	-3.24	**.001**	-.15	-1.6	.11	.26
Machiavellismi	-.04	-.61	.55	.02	.34	.73	.58
Narsismi	.15	2.29	**.02**	.06	.89	.38	.52
Psykopatia	.15	2.51	**.01**	.07	1.10	.27	.58

3.3 Polkumallit

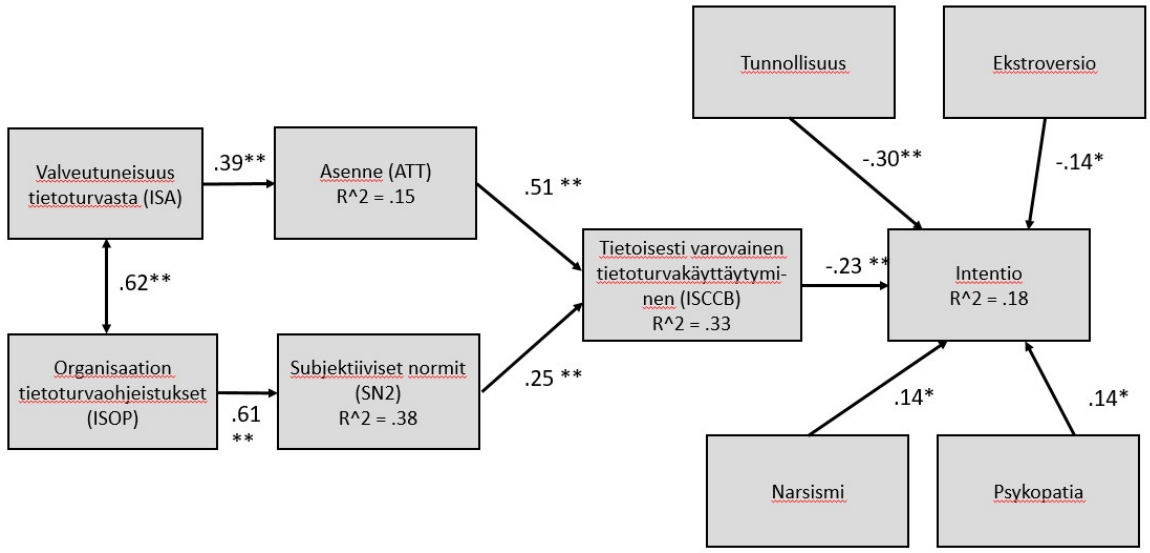
Polkumalleilla tarkasteltiin, toteutuuko aineistossa mittausmallin (kuva 2) mukainen teoreettinen rakenne. Mallia sovitettiin erikseen intentiolle (malli 1) ja asenteelle (malli 2), ryhmittelevänä muuttujana käytettiin luvussa 3.1 vaarallisuusasteeltaan erilaisia skenaariotilanteita niin, että ryhmä 1 käsitti matalamman riskin skenaariot ja ryhmä 2 puolestaan vakavamman riskin skenaariot.

Taulukko 5. Mallissa 1 tietoturvakäyttäytymisen muuttujilla ennustettiin intentiota skenaariotilanteessa, mallissa 2 asennetta tekoa kohtaan.

	RMSEA (90 % luottamusväli)	TLI	CFI	χ^2 (df)	χ^2 / df
Malli 1, ryhmä 1	0.17 (.16; .19)	.56	.67	137 (58)	2.34
Malli 1, ryhmä 2	0.17 (.16; .19)	.56	.67	262 (58)	4.52
Malli 2, ryhmä 1	0.17 (0.15;0.19)	.63	.74	72 (38)	1.89
Malli 2, ryhmä 2	0.17 (0.15;0.19)	.63	.74	195 (38)	5.13

Ryhmä 1 = vähäisen riskin skenaariotilanne, ryhmä 2 = vakavamman riskin skenaariotilanne

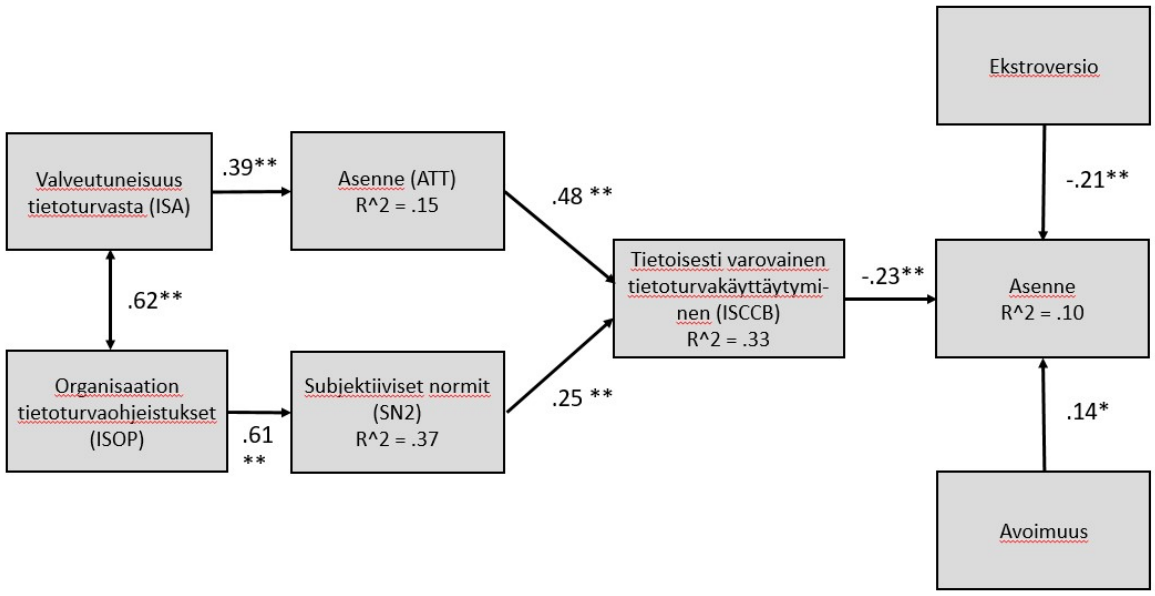
Malliin 1 sisällytetyt persoonallisuustekijät olivat tunnollisuus, ekstroversio, psykopatia ja narsismi, sillä nämä osoittautuivat regressioanalyysissä merkitseviksi intention ennustajiksi (taulukko 4). Mallin yhteensopivuusindeksit indikoivat heikkoa yhteensopivuutta kummassakin ryhmässä (taulukko 5). Mallissa 2 ryhmän 1 osalta khii toiseen -testisuureen ja vapausasteiden osamäärä alittaa kuitenkin arvon 2, jota on pidetty nyrkkisääntönä yhteensopivuuden ylärajalle (Tabachnick & Fidell, 2014, s. 770). Ryhmässä 1 päästiin kuitenkin lähelle tätä raja-arvoa, minkä takia kuvassa 5 on esitetty mallin parametrit.



Kuva 5. Standardoidut parametrit mallissa 1 ryhmälle 1. * p< .05 **, p<.001,

Mallin kaikki parametrit osoittautuivat merkitseviksi. Asenne ennusti subjektiivisia normeja vahvemmin sitä, miten varovasti henkilö koki toimivansa tietoturvan suhteen, yhdessä ne selittivät 33 % varovaisuusmuuttujan vaihtelusta. Tällä puolestaan oli merkitsevä (p<.001) ja negatiivinen yhteys intentiomuuttujaan skenaariotilanteessa. Mitä varovaisemmaksi henkilö siis arvioi itsensä, sitä epätodennäköisemmin hän koki toimivansa skenaariossa kuvatulla tavalla. Kaikki persoonallisuustekijät olivat yhteydessä skenaariotilanteen intentionmuuttujaan. Tunnollisuuden ja ekstroversion yhteys intentioon oli negatiivinen, narsismin ja psykopatian osalta tämä puolestaan oli positiivinen. Vahvin yhteys oli tunnollisuudella ($\beta = -.30$, p<.001). Yhdessä kaikki persoonallisuustekijät sekä tietoinen varovaisuus selittivät 18 % skenaariotilanteen intentiomuuttujasta. Mallin yhteensopivuus oli kuitenkin kaikkien indeksien perusteella heikko, eikä mittausmallin mukainen rakenne selittänyt siis tarpeeksi aineiston vaihtelusta.

Mallissa 2 tarkastellut persoonallisuustekijät olivat ekstroversio ja avoimuus, sillä niillä oli merkitsevä yhteys asennemuuttujaan regressioanalyysissä (taulukko 4). Mallin yhteensopivuusindeksit on esitetty taulukossa 4. Mallin sopivuus aineistoon oli heikko, mutta ryhmän 1 suhteen khii toiseen -testisuureen ja vapausasteiden osamäärä alitti arvon 2. Kuvassa 6 on mallin 2 tunnusluvut ryhmän 1 suhteen.



Kuva 6. Standardoidut parametrit mallissa 2 ryhmälle 1. * p< .05 **, p<.001.

Lähes kaikki parametrit olivat samansuuruisia mallissa 2 kuin kuvassa 5 esitetyssä mallissa 1 ja ne kaikki osoittautuivat merkitseviksi. Valveutuneisuusmuuttuja selitti tietoturva-asenne-muuttujan vaihtelusta 15 %. Organisaation tietoturvaohjeistukset puolestaan selittivät subjektiivisten normien vaihtelusta 37 % ja yhteys näiden välillä oli melko voimakas (β=.61, p<.001). Valveutuneisuus- ja tietoturvaohjeistusmuuttujien jakama kovarianssi oli niin ikään melko voimakasta ja merkitsevä (σ^2 = .62, p<.001). Asenne (β = .48, p<.001) oli subjektiivisia normeja (.25, p<.001) voimakkaampi selittäjä tietoisesti varovaiselle tietoturvakäyttäytymiselle, jonka vaihtelusta nämä selittivät yhteensä 33 %. Tämä varovaisuusmuuttuja oli puolestaan negatiivisesti yhteydessä skenaariotilanteen asennemuuttujaan. Kumpikin persoonallisuuspiirre osoittautui merkitseväksi selittäjäksi asennemuuttujalle, näistä voimakkaammin ekstroversio negatiivisesti (β = -.21, p<.001). Avoimuuden yhteys asenteeseen puolestaan oli positiivinen (β = .14, p<.05).

4 DISKUSSIO

Tämän tutkimuksen tarkoituksena oli skenaarioasetelman avulla selvittää, onko persoonallisuuden eri piirteillä vaikutusta siihen, miten todennäköisesti henkilö arvioi toimivansa tietoturvan vaarantavalla tavalla intentioina ja asenteina arvioituna. Lisäksi tarkasteltiin, voi-

daanko tällaista toimintaa ennustaa Ajzenin ja Fishbeinin (1975) perustellun toiminnan teorian (TRA) mukaisilla muuttujilla. Kiinnostuksen kohteena oli kuvassa 3 esitetty mittausmalli, jota tarkasteltiin esitettyjen skenaarioiden kahdella eri vaarallisuustasolla.

Tutkimuksen osallistujille annettiin luettavaksi skenaariotilanteita, joiden suhteen he arvioivat todennäköisyyttään toimia kuvatulla tavalla (intentio) sekä suhtautumistaan kuvattuun tekoon (asenne). Hypoteesien 3a ja 3b mukaisesti aineisto jakaantui näiden suhteen kahteen ryhmään – lievän haitan skenaarioihin ja vakavan haitan skenaarioihin, joista jälkimmäisessä sekä intentio että asenne olivat matalampia. Vain osa tutkimuksen aineistosta noudatti mittausmallin mukaista rakennetta. Perustellun toiminnan teorian mukaiset muuttujat olivat yhteydessä tietoisesti varovaiseen tietoturvakäyttäytymiseen, joka yhdessä persoonallisuustekijöiden kanssa oli yhteydessä skenaariotilanteen asenteisiin silloin, kun kiinnostuksen kohteena oli lievemmän haitan skenaariot. Korkeampi valveutuneisuus oli yhteydessä myönteisempään tietoturva-asenteeseen ja organisaation selkeämpi ja myönteisempi suhtautuminen tietoturvaan oli varsin voimakkaasti yhteydessä siihen, että vastaaja koki niiden vaikuttavan toimintaansa. Yhdessä nämä yksilön kokemat subjektiiviset normit ja tietoturva-asenne selittivät yksilön arviota omasta harkitsevasta tietoturvakäyttäytymisestään noin kolmanneksen. Havaitut yhteydet olivat samansuuntaisia, mutta pääasiallisesti heikompia kuin Safan ym. (2015) alkuperäistutkimuksessa, lukuun ottamatta tietoturvaohjeistuksien yhteyttä subjektiivisiin normeihin, joka oli hieman voimakkaampi. Tämä rakenne oli siis TRA:n mukainen ja aineiston tältä osalta linjassa hypoteesin 1 kanssa, mikä tukee perustellun toiminnan teorian käyttöä tietoturvakäyttäytymisen tutkimuksessa. Tietoisesti varovaisempi toiminta tietoturvan suhteen oli puolestaan yhteydessä kielteisempään asenteeseen esitettyä tilannetta kohtaan. Tämä antaisi viitteitä siitä, että TRA:lla voidaan ennustaa toimintaa myös konkreettisessa tilanteessa, ja että asenteisiin spesifeissä tilanteissa voidaan vaikuttaa lisäämällä valveutuneisuutta ja kokemusta normeista esimerkiksi tietoturvaohjeistuksin ja -koulutuksin. Tulos on rohkaiseva tietoturvarikkeiden ehkäisyn kannalta, sillä se antaa viitteitä siitä, että myös lievempiin rikkomuksiin voitaisiin vaikuttaa näillä keinoilla.

Tietoturvaa enemmän vaarantavien skenaarioiden osalta aineisto ei kuitenkaan noudattanut mittausmallin mukaista rakennetta ja lievempienkin tilanteiden tietoturvaintentioiden suhteen päästiin vain lähelle yhteensopivuutta. Tietoturvan kannalta vaarallisempien toimien taustalla saattaa siis olla erilainen taustamuuttujien rakenne kuin tämän tutkimuksen mittausmallissa. Tämä on mielenkiintoinen tulos, sillä aiemmassa tutkimuksessa tekojen erilaista vaarallisuus-

tasoa ei ole hyödynnetty koeasetelmissa. Mittausmallin rakenne ei myöskään toteutunut silloin, kun kiinnostuksen kohteena oli intentio skenaariotilanteessa. Tulos on yllättävä, sillä TRA:n uskottiin ennustavan intentiota samalla tavoin kuin asennettakin. Tähän tulokseen on saattanut vaikuttaa vähäinen hajonta intentioissa, sillä vain pieni osa vastaajista raportoi, että olisi saattanut toimia kuvatulla tavalla. Pyrkimys vastata sosiaalisesti suotavalla tavalla lienee vahvistaneen tätä. Tietoturvakäyttäytymisen tutkimuksessa käytettyjä teorioita on lukuisia (Moody ym., 2018), ja myöhemmän tutkimuksen selvitettäväksi jää, sopisiko jokin muu teoria selittämään ilmiötä.

Yhtenä tutkimuksen kiinnostuksen kohteista oli, onko persoonallisuuden piirteillä yhteyttä vastaajan intentioon ja asenteeseen skenaariotilanteessa. Tarkastelun kohteena olivat viiden suuren piirteen teoria sekä Dark Triad -teoria. Aiemman tutkimuksen (esim. Shropshire ym., 2015) perusteella asetettiin hypoteesi 4a, jonka mukaan tunnollisimmat ja sovinnollisimmat vastaajat arvioisivat todennäköisyytensä toimia kuvatulla tavalla pienimmäksi, sekä asenteensa tätä kohtaan kielteisimmäksi. Hypoteesin vastaisesti tällaista yhteyttä ei kuitenkaan havaittu, ja tunnollisuus oli yhteydessä ainoastaan intentioon. Tällöinkin huomion arvoista oli, että suurin osa vastaajien tunnollisuudesta oli selitettävissä muilla persoonallisuuden piirteillä, mikä oli yllättävää, sillä käsitys viidestä piirteestä on vakiintunut. Viidestä suuresta persoonallisuuden piirteestä sen sijaan ekstroversiolla havaittiin negatiivinen yhteys sekä intentioon että asenteeseen. Lisäksi vastaajan korkeampi avoimuus uusille kokemuksille oli yhteydessä myönteisempään suhtautumiseen skenaariotilannetta kohtaan. Ekstroversion ja avoimuuden yhteyttä asenteeseen tarkasteltiin myös tutkimuksen mittausmallissa, jossa yhteydet säilyivät samansuuntaisina. Yhdessä tietoisesti varovaisen tietoturvakäyttäytymisen kanssa ne ennustivat asenteen vaihtelusta kymmeneksen. Ekstroversion ja avoimuuden yhteys tässä tutkimuksessa tarkasteltuun tietoturvakäyttäytymiseen oli yllättävä, sillä perinteisesti näitä piirteitä ei ole nähty mielekkäinä ennustajina tietoturvassa. Avoimuuden positiivinen yhteys lienee ymmärrettävissä heijasteena avoimuutena uusille toimintatavoille. Viiden suuren piirteen yhteys tietoturvakäyttäytymiseen lienee siis oletettua moninaisempaa ja tämä tulos antaa viitteitä siitä, että näiden piirteiden poisjättö ei välttämättä ole aina perusteltua.

Toisena tarkasteltuna piirreteoriana oli Dark Triad -teoria, jonka piirteiden yhteyttä tietoturvakäyttäytymiseen ei aiemmin ole tutkittu. Kirjallisuuteen perustuen asetettiin hypoteesi 4b, jonka mukaan nämä kolme piirrettä olisivat positiivisesti yhteydessä intentioihin ja asenteisiin. Hypoteesin vastaisesti Machiavellismilla ei ollut yhteyttä kumpaankaan, eikä mikään

kolmesta piirteestä ollut yhteydessä tietoturva-asenteisiin skenaariotilanteessa. Sen sijaan voimakkaammat narsismi ja psykopatia olivat yhteydessä korkeampaan vastaajan arvioimaan todennäköisyyteen syyllistyä kuvattuun tietoturvarikkeeseen. Tulos on linjassa aiemman tutkimuksen kanssa, jossa Dark Triad -piirteiden on havaittu ennustavan yleisesti haitallista toimintaa työpaikalla (Deshong, Grant & Mullins-Sweatt, 2015; Scherer, Baysinger, Zolynsky & Lebreton, 2013). Tämä tutkimus antaa viitteitä siitä, että vastaava yhteys olisi löydettävissä myös spesifimmin tietoturvakäyttäytymisen suhteen. Näiden piirteiden yhdistäminen tietoturvakäyttäytymisen tutkimukseen on ollut vähänlaista, minkä takia niiden tarkastelu tässä tutkimuksessa tarjoaa mahdollisuuksia uusiin johtopäätöksiin. Dark Triad -piirteiden erillisyydestä on ollut keskustelua (Book ym., 2015), mutta tämän tutkimuksen perusteella niillä vaikuttaisi ainakin tietoturvakäyttäytymisen osalta olevan itsenäinen selitysvoima, sillä piirteiden välillä ei havaittu liiallisesti yhteisvaihtelua. Samalla tulos tukee ajatusta siitä, että viisi suurta piirrettä eivät välttämättä kata kaikkia persoonallisuuden puolia. Viiden suuren tilalle onkin myös ehdotettu kuuden persoonallisuuden piirteen mallia (Lee, Ashton, Morrison, Cordery & Dunlop, 2008). Vaikka tämä tutkimus ei vastaa kysymykseen siitä, montako piirrettä olisi oikea määrä, se antaa viitteitä siitä, että aihetta olisi hyvä tarkastella vielä tulevissa tutkimuksissa.

Tämän tutkimuksen vahvuutena voidaan nähdä tutkimusote, jolla pyrittiin täydentämään puutteita aiemmassa tietoturvakäyttäytymisen tutkimuksessa. Skenaarioasetelma mahdollisti käyttäytymisen tarkastelun hieman lähempänä todellista käyttäytymistä kuin tavanomainen kyselytutkimus. Eri vaarallisuusasteisia skenaarioita hyödyntämällä saatiin myös viitteitä siitä, että vaarallisuudeltaan erilaisten tietoturvarikkeiden taustalla voi olla erilaisia tekijöitä, minkä tarkastelu olisikin tärkeää jatkotutkimuksen kannalta. Persoonallisuuden tarkastelun yhdistäminen tutkimusasetelmaan mahdollisti lisäksi kokonaisvaltaisemman tietoturvakäyttäytymisen tarkastelun. Vahvuutena voidaan myös nähdä Dark Triad -inventaarin suomentaminen ja käyttöönotto tietoturvakäyttäytymisen tutkimuksessa. Näiden piirteiden yhteydestä tietoturvakäyttäytymiseen ei aiemmin ollut juurikaan tutkimusta, mutta tässä tutkimuksessa saatujen tulosten perusteella niiden huomiointi jatkotutkimuksessa on perusteltua. Tietoturvan taustalla vaikuttavien persoonallisuustekijöiden tunteminen on tärkeää, sillä niistä voi olla hyötyä esimerkiksi ohjeistusten suunnittelussa, kuten Kajzerin ja muiden (2014) tutkimuksessa. Lisäksi niiden tunteminen mahdollistaa persoonallisuuden huomioinnin jo esimerkiksi rekrytointitilanteessa.

Tutkimuksen rajoitteiksi voidaan mainita painottunut otos, joka korkeakoulutaustan ja -valintojen johdosta painottuu nuoreen ja mahdollisesti persoonallisuudeltaan valtaväestöä hieman erilaiseen populaatioon. Lienee mahdollista, että esimerkiksi Maanpuolustuskorkeakoulusta on valintavaiheessa karsiutunut pois henkilöitä, joilla Dark Triad -piirteet ovat korkeita. Vastaajien nuori ikä on niin ikään saattanut heijastua vastauksiin korkeampana tietoutena tietoturvaan liittyvistä asioista niin sanotun diginatiiviuuden johdosta mikä johtaa siihen, etteivät tulokset todennäköisesti täysin yleisty koko työväestöön. Lisäksi rajoitteena voidaan mainita heikko erottelukyky osassa käytettyjä inventaareja, sillä tietoturvakäyttäytymistä tarkastelevissa kysymyksissä osallistujat vastasivat pääasiassa hyvän tietoturvakäytänteen mukaisesti ja vastaukset jakaantuivat siten vinosti. Kyselytutkimukseen liittyvät sosiaalisesti suotavan vastaamisen ongelmat ovat saattaneet korostua erityisesti Dark Triad -inventaarin suhteen, jossa osa väittämistä kartoittaa arkaluontoista tietoa.

Tämä tutkimus yhdisti uudella tavalla yksilön ja organisaation tekijöiden tarkastelua tietoturvakäyttäytymisen taustalla. Saadut tulokset antavat tukea sille, että persoonallisuustekijöiden kartoitus on tietoturvakäyttäytymisen yhteydessä hyödyllistä, ja että myös epärehellistä persoonallisuutta tarkastelevat inventaarit tulisi yhdistää alan tutkimukseen. Perustellun toiminnan teorialla ei pystytty selittämään rakennetta koko aineistossa, mikä tarjoaa mahdollisuuksia tarkastella muita teorioita tulevissa tutkimuksissa ja mikäli nämä selittävät erityisesti vaarallisia tietoturvarikkeitä. Tulokset kuitenkin osoittavat, että niin organisaation tarjoamilla tietoturvaohjeistuksilla, yksilön valveutuneisuudella kuin persoonallisuudellakin on paikkansa tietoturvan vahvistamisessa.

5 KIRJALLISUUS

Achen, C. H. & Snidal, D. (1989). Rational Deterrence Theory and Comparative Case Studies. *World Politics*, *41*(2), 143–169.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behaviour and Human Decision Processes*, *50*, 179–211.

Alaskar, M., Vodanovich, S. & Shen, K. N. (2015). Evolvement of Information Security Research on Employees' Behavior: A Systematic Review and Future Direction. *2015 48th Hawaii International Conference on System Sciences*, 4241–4250. http://doi.org/10.1109/HICSS.2015.508

Book, A., Visser, B. A. & Volk, A. A. (2015). Unpacking "evil": Claiming the core of the Dark Triad. *Personality and Individual Differences*, *73*, 29–38. http://doi.org/10.1016/j.paid.2014.09.016

Chang, M. K. (1998). Predicting Unethical Behavior : A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior. *Journal of Business Ethics*, *17*, 1825–1834.

Deshong, H. L., Grant, D. M. & Mullins-Sweatt, S. N. (2015). Comparing models of counterproductive workplace behaviors: The Five-Factor Model and the Dark Triad. *Personality and Individual Differences*, *74*, 55–60. http://doi.org/10.1016/j.paid.2014.10.001

Ehrenfeld, J. M. (2017). WannaCry , Cybersecurity and Health Information Technology : A Time to Act, 10916. http://doi.org/10.1007/s10916-017-0752-1

Funder, D. C. (2006). Towards a resolution of the personality triad: Persons, situations, and behaviors. *Journal of Research in Personality*, *40*(40), 21–34. http://doi.org/10.1016/j.jrp.2005.08.003

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier Scientific Publishing Company.

Goldberg, L. R. (1990). An Alternative "Description of Personality": The Big-Five Factor Structure. *Journal of Personality and Social Psychology*, *59*(6), 1216–1229.

Guo, K. H., Yuan, Y., Archer, N. P. & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of*

Management Information Systems, *28*(2), 203–236. http://doi.org/10.2753/MIS0742-1222280208

Hox, J. J., Maas, C. J. M. & Brinkhuis, M. J. S. (2010). The effect of estimation method and sample size in multilevel structural equation modeling, *64*(2), 157–170. http://doi.org/10.1111/j.1467-9574.2009.00445.x

Jones, D. N. & Paulhus, D. L. (2014). Introducing the Short Dark Triad (SD3): A brief measure of dark personality traits. *Assessment*, *21*(1), 28–41. http://doi.org/10.1177/1073191113514105

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A. & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security*, *43*, 64–76. http://doi.org/10.1016/j.cose.2014.03.003

Konstabel, K., Lönnqvist, J.-E., Walkowitz, G., Konstabel, K. & Verkasalo, M. (2012). The ' Short Five ' (S5): Measuring Personality Traits Using Comprehensive Single Items. *European Journal of Personality*, *26*, 13–29. http://doi.org/10.1002/per

Lee, K. & Ashton, M. C. (2004). Psychometric Properties of the HEXACO Personality Inventory. *Multivariate Behavioral Research*, *39*(2), 329–358. http://doi.org/10.1207/s15327906mbr3902_8

Lee, K., Ashton, M. C., Morrison, D. L., Cordery, J. & Dunlop, P. D. (2008). Predicting integrity with the HEXACO personality model: Use of self- and observer reports. *Journal of Occupational and Organizational Psychology*, (81), 147–167. http://doi.org/10.1348/096317907X195175

Maasberg, M., Warren, J. & Beebe, N. L. (2015). The Dark Side of the Insider : Detecting the Insider Threat Through Examination of Dark Triad Personality Traits. Teoksessa *48th Hawaii International Conference on System Sciences* (ss. 3518–3526). Kauai, HI: IEEE. http://doi.org/10.1109/HICSS.2015.423

McCrae, R. R. & Costa, P. T. (1987). Validation of the Five-Factor Model of Personality Across Instruments and Observers. *Journal of Personality and Social Psychology*, *52*(1), 81–90.

Moody, G. D., Siponen, M. & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311.

http://doi.org/10.25300/MISQ/2018/13853

Paulhus, D. L. & Williams, K. M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, *36*, 556–563.

Pfleeger, S. L., Predd, J. B., Hunker, J. & Bulford, C. (2010). Insiders Behaving Badly: Addressing Bad Actors and Their Actions. *IEEE Transactions on Information Forensics and Security*, *5*(1), 169–179. http://doi.org/10.1109/TIFS.2009.2039591

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78. http://doi.org/10.1016/j.cose.2015.05.012

Scherer, K. T., Baysinger, M., Zolynsky, D. & Lebreton, J. M. (2013). Predicting counterproductive work behaviors with sub-clinical psychopathy: Beyond the Five Factor Model of personality. *Personality and Individual Differences*, *55*, 300–305. http://doi.org/10.1016/j.paid.2013.03.007

Shropshire, J., Warkentin, M. & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. http://doi.org/10.1016/j.cose.2015.01.002

Siponen, M. & Vance, A. (2010). Neutralization: New Insights of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *28*(3), 337–362. http://doi.org/10.2460/javma.228.4.578

Sohrabi Safa, N., Von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13. http://doi.org/10.1016/j.cose.2015.10.006

Sommestad, T. & Hallberg, J. (2013). A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance, 257–271.

Tabachnick, B. G. & Fidell, L. S. (2014). *Using Multivariate Statistics. Pearson New International Edition* (6. p.). Pearson Education Limited.

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. http://doi.org/10.1016/j.im.2012.04.002

Vashisth, A. & Kumar, A. (2013). Corporate espionage: The insider threat. *Business Information Review*, *30*(2), 83–90. http://doi.org/10.1177/0266382113491816

Wiltshire, J., Bourdage, J. S. & Lee, K. (2014). Honesty-Humility and Perceptions of Organizational Politics in Predicting Workplace Outcomes. *Journal of Business and Psychology*, *29*, 235–251. http://doi.org/10.1007/s10869-013-9310-0

Woon, I. M. Y. & Kankanhalli, A. (2007). Investigation of IS professionals ' intention to practise secure development of applications. *International Journal of Human-Computer Studies*, *65*, 29–41. http://doi.org/10.1016/j.ijhcs.2006.08.003

6 LIITTEET

Liite 1. Kyselylomakkeen suomennetut osiot, keskiarvot ja keskihajonnat

Short Dark Triad			
Machiavellismi		**Ka**	**Kh**
Ma1	On hyvä saada merkittäviä ihmisiä omalle puolelle keinoja kaihtamatta.	2.15	1.1
Ma2	On hyvä pitää kirjaa tiedoista, joita voi tulevaisuudessa käyttää toisia ihmisiä vastaan.	1.48	0.85
Ma3	Ei ole viisasta kertoa omia salaisuuksia toisille.	3.16	1.21
Ma4	Suoria konflikteja muiden kanssa tulee välttää, koska heistä voi olla hyötyä tulevaisuudessa	3.08	1.18
Ma5	On hyvä odottaa sopivaa hetkeä koston toteuttamiselle.	1.83	1.08
Ma6	Tykkään manipuloida toisia saavuttaakseni tavoitteeni.	1.43	0.8
Ma7	Pidä huoli, että suunnitelmasi hyödyttävät sinua eivätkä muita.	1.27	0.58
Ma8	Joitain asioita on hyvä salata muilta ihmisiltä maineensa suojaamiseksi.	3.64	1.07
Ma9	Suurin osa ihmisistä on manipuloitavissa.	2.91	1.26
Narsismi			
Na1 (R)	Vihaan huomion keskipisteenä olemista.	3.21	1.18
Na2	Ihmiset näkevät minut luontaisena johtajana.	3.04	1.27
Na3	Suurin osa ryhmäaktiviteeteista olisi tylsiä ilman minua.	2.33	1.09
Na4 (R)	Olen keskivertoihminen.	2.85	1.2
Na5	Vaadin saada kunnioitusta, joka minulle kuuluu.	3.02	1.16

Na6	Tykkään tehdä tuttavuutta merkittävien ihmisten kanssa.	2.99	1.15
Na7	Minua on verrattu kuuluisiin ihmisiin.	2.06	1.15
Na8	Tiedän olevani erityinen, koska kaikki sanovat niin.	1.96	0.99
Na9 (R)	Tulen kiusaantuneeksi, jos joku kehuu minua.	3.1	1.19
Psykopatia			
Ps1	Nautin seksistä ihmisten kanssa, joita hädin tuskin tunnen.	2.33	1.35
Ps2	Ihmiset, jotka sekaantuvat asioihini, katuvat sitä.	2.02	0.97
Ps3	On totta, että olen joskus ilkeä toisia kohtaan.	2.74	1.25
Ps4	Sanon mitä tahansa, jotta saan haluamani.	1.54	0.76
Ps5 (R)	En ole koskaan joutunut ongelmiin virkavallan kanssa.	1.62	1.15
Ps6 (R)	Välttelen vaarallisia tilanteita.	2.58	1.19
Ps7	Koston tulee olla pikainen ja ilkeä.	1.58	0.91
Ps8	Pidän siitä, kun voin kostaa auktoriteeteille.	1.61	0.98
Ps9	Ihmiset sanovat usein, että käyttäydyn hallitsemattomasti.	1.34	0.70

Tietoturvakäyttäytyminen		Ka	Kh
Tietoisesti varovainen tietoturvakäyttäytyminen			
ISCCB1	Mietin tekojeni seurauksia, ennen kuin teen mitään tietoturvaan vaikuttavaa.	4.13	0.88
ISCCB2	Keskustelen tietoturva-asiantuntijoiden kanssa, ennen kuin teen mitään tietoturvaan liittyvää.	2.42	1.16

ISCCB3	Otan huomioon tietoturva-asiantuntijoiden suositukset toimintatavoissani.	4.06	0.89
ISCCB4	Otan huomioon aiemmat kokemukseni tietoturvasta, jotta vältän aikaisempien virheiden toistamisen.	4.5	0.71
ISCCB5	Yritän jatkuvasti muuttaa tietoturvakäyttäytymistäni tietoisesti varovaisemmaksi.	3.65	1.04
Organisaation tietoturvaohjeistukset			
ISOP1	Oppilaitoksessani arvostetaan tietoturvaohjeistuksien ja -käytäntöjen mukaan toimimista.	4.09	0.92
ISOP2	Tietoturvaohjeistukset ja -käytännöt vaikuttavat toimintaani.	4.13	0.89
ISOP3	Tietoturvaohjeistukset ja -käytännöt ovat kiinnittäneet huomioni.	3.65	1.12
ISOP4	Tietoturvaohjeistukset ja -käytännöt ovat tärkeitä oppilaitoksessani.	3.95	1.01
Asenne tietoturvaa kohtaan			
ATT1	Tietoinen varovaisuus tietoturvan suhteen on suositeltavaa.	4.68	0.58
ATT2	Minulla on myönteinen näkemys käyttäjien tietoturvakäyttäytymisen kehittymisestä varoivaisempaan suuntaan.	3.6	0.95
ATT3	Uskon, että tietoisesti varovainen tietoturvakäyttäytyminen on arvokasta oppilaitoksissa.	4.41	0.66
ATT4	On hyödyllistä toimia tietoisen varovaisesti tietoturvaan liittyvissä asioissa.	4.38	0.78
ATT5	Tietoinen varovaisuus tietoturvan suhteen on välttämätöntä.	4.38	0.72
Subjektiiviset normit			
SN1	Opettajani/ohjaajani tietoturvakäyttäytyminen vaikuttaa omaan toimintaani.	2.81	1.29
SN2	Oppilaitokseni tietoturvakulttuuri vaikuttaa toimintaani.	3.63	1.16

SN3	Opiskelutovereitteni tietoturvakäyttäytyminen vaikuttaa omaan toimintaani.	2.69	1.23
SN4	Tietoturvaohjeistukset ovat tärkeitä opiskelutovereilleni.	3.1	0.99
Valveutuneisuus tietoturvasta			
ISA1	Ymmärrän riskit tietoturvallisuudessa.	4.28	0.84
ISA2	Minulla on riittävästi tietoa tietoturvarikkeiden kustannuksista.	2.82	1.33
ISA3	Olen tietoinen mahdollisista tietoturvauhkista.	4.03	0.93
ISA4	Pidän itseni ajan tasalla tietoturvaan liittyvistä asioista.	3.31	1.15

Liite 2. Skenaariot

Paketti 1. Vakava riski tai tietoturvarikkomus

Suojatun aineiston käyttö

Antti saa opintojaan varten käyttöönsä luottamuksellista aineistoa, joka sisältää yksityishenkilöiden vastauksia henkilökohtaisiin ja arkaluontoisiin kysymyksiin. Aineistoa ei ohjeiden mukaan saa esitellä tai luovuttaa toisille osapuolille, sillä se sisältää henkilösuojalain alaisia tietoja. Osa vastauksista on hyvinkin mielenkiintoisia ja Antti päättää näyttää ne tyttöystävälleen.

Työkoneen käyttö muuhun tarkoitukseen

Jussi on työharjoittelussa. Jussi saa käyttöönsä työnantajan kannettavan tietokoneen, jota tulee käyttää vain työtehtävien toteuttamiseen. Työnantajan kone on Jussin omaa konetta huomattavasti uudempi. Viikonloppuna Jussi lataa koneelle tietokonepelejä, joita ei omalla koneellaan voi käyttää koneen heikon tehon takia. Jussi poistaa asennukset maanantaina.

Sama salasana useissa palveluissa

Milja käyttää päivittäin yliopistonsa sähköpostia sekä omaa yksityistä sähköpostiaan. Lisäksi hän on aktiivinen Facebookin, Twitterin ja Instagramin käyttäjä. Milja myös viikoittain katsoo puhelimensa mobiilisovelluksen kautta pankkitilinsä saldon, jotta hän pystyy seuraamaan tilinsä tapahtumia. Milja käyttää salasanaa “Kop95ReT” kaikissa edellä mainittujen palvelujen käyttäjätunnuksissa.

Paketti 2. Kohtalainen riski tai tietoturvarikkomus

Helppo salasana

Mikael on juuri aloittanut yliopiston, ja hänen täytyy keksiä salasana yliopiston intranet-käyttäjätunnusta varten. Hän luo salasanakseen “Mikael1”. Toisena opiskeluvuonna, kun järjestelmä pyytää häntä vaihtamaan salasanansa, Mikael valitsee salasanakseen “Mikael2”. Kolmantena opiskeluvuotena järjestelmä pyytää jälleen vaihtamaan salasanan, jolloin Mikael vaihtaa salasanakseen “Mikael3”.

Löytynyt USB tikku

Oskari on matkalla oppilaitoksensa ATK-luokkaan ja löytää maasta nimettömän USB-muistitikun. Selvittääkseen kenelle tikku mahdollisesti kuuluu, hän tökkää sen yhteen oppilaitoksen koneista katsoakseen mitä se sisältää.

Tein, koska muutkin tekivät

Anna on tekemässä ryhmätyötä ryhmässä, jossa osa jäsenistä on hänen ystäviään. Työn tekemistä varten tarvitaan ohjelma, joka on opiskelijoille ilmainen vain oppilaitoksen koneilla. Anna asuu kauempana oppilaitoksesta, joten hänen aikaansa säästäisi huomattavasti, jos hän saisi tehtyä työtä kotoaan käsin. Omaan koneeseen ladattuna ohjelma maksaa kuitenkin joitain kymmeniä euroja. Annan ystävät ryhmässä näyttävät hänelle sivun, josta ovat saaneet ohjelman ladattua ilmaiseksi torrent-tiedostona. Anna päättää ladata ohjelman tätä kautta.

Paketti 3. Vain vähäinen riski tai tietoturvarikkomus

Arvonnan jakaminen

Jaakko on aktiivinen facebookin käyttäjä. Eräänä iltana hän huomaa etusivullaan julkaisun liittyen arvontaan, johon osallistuminen kiinnostaa Jaakkoa: Mahdollisuus voittaa 3000 euron lahjakortti Ebay:hin! Arvontaan osallistuminen vaatii ilmoituksen jakamista eteenpäin. Jaakko päättää jakaa ilmoituksen seinällään, sen tarkemmin tutkimatta arvontaa mainostavaa sivustoa.

Wi-fi ulkomailla

Mikko on matkustamassa ulkomailla. Hän on etukäteen suunnitellut menevänsä hyväksi kehuttuun ravintolaan, mutta unohtanut kirjoittaa sen tarkan osoitteen ylös. Kierreltyään alueella hetken oikeaa paikkaa löytämättä Mikko päättää tarkistaa, oliko lähistöllä avoimia wifi-verkkoja, jotta hän voisi nopeasti hakea ravintolan osoitteen netistä. Mikko löytää avoimen verkon ja päättää yhdistää siihen. Hän saa nopeasti etsittyä osoitteen ja kirjautuu sitten ulos verkosta.

Tietokoneen lukitsematta jättäminen

Marja tekee opintoihin liittyvää ryhmätyötä kolmen hengen ryhmässä. Ryhmä työskentelee koulun koneella kirjautuneen Marjan tunnuksilla. Marja joutuu lähtemään seuraavalle oppitunnille ja tietoturvaohjeistuksen vastaisesti jättää kirjautumatta ulos tietokoneelta, jotta muut ryhmän jäsenet voivat jatkaa työskentelyä hänen poissa ollessaan.